مخاطر نظم المعلومات المحاسبية الإلكترونية
في الشركـــات الماليــة الأردنيـة
(البنوك وشركات التأمين)

إعداد
أمجد يوسف إسماعيل الزعاترة

إشراف
الدكتور وليد زكريا صيام
أستاذ مشارك

قدمت هذه الرسالة استكمالاً لمتطلبات درجة الماجستير

في تخصص المحاسبة والتمويل

عمادة البحث العلمي والدراسات العليا في الجامعة الهاشمية

الزرقاء - الأردن

١٠/ ٥ / ٢٠١١م

نوقشت هذه الرسالة واجيزت بتاريخ 10/ 5 / 2011م

أعضاء لجنة المناقشة	التوقيـــــع
د. وليد زكريـــا صيـــام، مشرفاً ورئيساً أستاذ مشارك – محاسبة إدارية	
د. حسام الدين مصطفى الخداش، عضواً أستاذ مشارك – نظرية محاسبية	
د. فهيم صـــالح لوندي، عضواً أستاذ مشارك – محاسبة مالية	
أ.د. يوسف مصطفى سعادة، عضواً أستاذ – محاسبــة تكاليف جامعــة العلوم التطبيقية	

الإهــــداء

إلى زوجتي العزيزة التي ساعدتني لإنجاز هذا العمل ....

إلى عائلتي التي ساندتني في الوصول إلى هذا الإنجاز ......

إلى أساتذتي وزملائي الذين ساعدوني على إنجاز هذه الرسالة...

وإلى كل من دعمني وساعدني لإنجاز هذا العمل ....

لهم جميعا أهدي ثمرة جهدي المتواضع....

شكر وتقدير

الحمد لله على إحسانه وتوفيقه، وعظيم شكري وتقديري لأهل الفضل لن أنسى فضلهم:

نبع العلم والعطاء أستاذي الفاضل الدكتور وليد زكريا صيام الذي غمرني برعايتـــه وتوجيهـــه حتى تم إنجاز هذه الرسالة، الأساتذة الكرام أعضاء لجنة مناقشة الرسالة، الأساتذة الكرام الـــذين قاموا بتحكيم إستبانة الدراسة وتقويمها، إلى كل من كان له يد فضلى في إنجاز هذا العمل.

أقدم شكري وتقديري

قائمة المحتويات

قائمة المحتويات

قائمة الجداول

قائمة الأشكال

قائمة الملاحق

ملخص

مخاطر نظم المعلومات المحاسبية الإلكترونية
في الشركـــــات الماليــــــــــة الأردنية
(البنوك وشركات التأمين)

إعداد
أمجد يوسف إسماعيل الزعاترة

المشرف
الدكتوروليد زكريا صيام
أستاذ مشارك

هدفت هذه الدراسة إلى التعرف على المخاطر التي تواجه نظـــم المعلومـــات المحاســـبية الإلكترونية في الشركات المالية الأردنية (البنوك وشركات التأمين)، والتعـــرف علـــى درجـــة تكرار حدوث هذه المخاطر وإجراءات الحماية التي تقوم بها إدارات البنوك وشـــركات التـــأمين للحد من وقوعها.

ولتحقيق أهداف الدراسة، تم تطوير إستبانة وتوزيعها على المديرين الماليين في البنـــوك وشركات التأمين الأردنية المدرجة في بورصة عمان لعام ٢٠٠٩م والبالغ عددها ١٥ بنكاً و ٢٨ شركة تأمين .

وقد بلغ عدد الإستبانات الموزعة (٤٣) إستبانة، تم استرداد واعتماد (٣٧) إســـتبانة لغايـــات التحليل الإحصائي، أي مانسبته (٨٦%) من إجمالي الإستبانات الموزعة، وقد تم التوصل إلـــى النتائج التالية :-

١- هناك العديد من المخاطر التي تهدد أمن المعلومات المحاسبية الإلكترونية في الـــشركات المالية الأردنية .
٢- تشكل المخاطر البيئية أكثر أنواع المخاطر التي تعاني منها الشركات المالية الأردنية.
٣- تعاني نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التأمين الأردنيـــة مـــن تكرار حدوث المخاطر التي تهدد أمن معلوماتها.
٤- هناك إهتمام كبير لدى القائمين على الشركات المالية الأردنية بتوفير نظام خاص لأمـــن المعلومات في الشركة.

وفي ضوء نتائج الدراسة تم التوصل إلى مجموعة من التوصيات من أهمها :-

١- ضرورة وضع إجراءات تضمن إستمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الازمات.
٢- تطبيق إستراتيجية الرقابة الوقائية لمنع وقوع الأخطاء أو المخالفات أو الحد منها في المرحلة الأولى من مراحل النظام .
٣- تطوير قدرات العاملين في مجال أمن المعلومات وحمايتها وزيادة الإهتمام بإشراكهم في الدورات المتخصصة في هذا المجال.

الفصل الأول

الإطار العام للدراسة

- مقدمة
- مشكلة الدراسة
- أهداف الدراسة
- أهمية الدراسة
- الدراسات السابقة
- فرضيات الدراسة

مقدمـــة:

أدى هذا التطور الهائل في تكنولوجيا المعلومات في الآونـــة الأخيـــرة إلـــى تطـــورات إقتصادية كبيرة وإلى مرحلة إنتقال مهمة في بيئة الأعمال ، فكبر حجم المـــشروعات وتنوعـــت أهدافها وظهرت الشركـــات متعددة الجنسيات وانتشرت التجارة الالكترونية ، وأصـــبح واجبـــاً على الشركات أن تستجيب بسرعة كبيرة لهذه التغيرات ومن أوجـــه الاســـتجابة التحـــول مـــن استخدام نظم المعلومات المحاسبية اليدوية إلى نظم المعلومات المحاسبية الإلكترونية ، التي توفر معلومات تتسم بالسرعة مع إمكانية الوصول إليها بسهولة من مواقع مختلفة، مما يتـــيح لـــلإدارة الحصول على المعلومات المطلوبة بالدقة والتوقيت الملائمين لتسهيل عملية التخطـــيط وإتخـــاذ القرار والمتابعة وحل المشاكل بكفاءة وفعالية.

ويتوجب على إدارة الشركة أن يتوفر لديها الفهم الجيد لنظم المعلومـــات الالكترونيـــة ومكوناتها والمخاطر التي تواجهها ، بحيث يساعد هذا الفهم في استخدام نظـــم المعلومـــات بمـــا يحقق أهداف الشركة .

من هنا جاءت فكرة هذه الرسالة للوقوف على طبيعة مخاطر نظم المعلومـــات المحاســـبية الإلكترونية في الشركات المالية الأردنية (البنـــوك وشـــركات التـــأمين) ودرجـــة تكرارهـــا وإجراءات الحماية التي تنتهجها هذه الشركات للحد من تأثيرات هذه المخاطر.

مشكلة الدراسة :

على الرغم مما توفره نظم المعلومات المحاسبية الالكترونية من مزايا وفوائد فإنها تنطوي على العديد من المخاطر التي يمكن أن تعود للأسباب التالية (Romney&Steinbart,2006,p190) :

١- إزدياد عدد أنظمة المعلومات مما أدى إلى أن تصبح المعلومات متاحة لعدد كبير جداً من الاشخاص .

٢- تعتبر السيطرة على الشبكات الإلكترونية المنتشرة بشكل كبير جداً أصعب بكثير من السيطرة على النظام اليدوي المركزي.

٣- الإنتشار الواسع للشبكات الإلكترونية مكّن الزبائن والمورّدين من الدخول إلى الأنظمة الإلكترونية ، مما جعل خصوصية المعلومات تحظى باهتمام كبير.

وبما أن النظام المحاسبي الإلكتروني يعتبر من أهم الأنظمة المنتجة للمعلومات التي تسهم في ترشيد ومساندة القرارات الإدارية والاقتصادية التي تؤثر على موارد المجتمعات وثرواتها وبالتالي على رفاهية أفرادها ، فقد جاءت هذه الدراسة للإجابة على التساؤلات التالية :-

١- ما طبيعة المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الأردنية؟

٢- ما درجة تكرار حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الأردنية؟

٣- ما إجراءات الحماية التي تتبعها الشركات المالية الأردنية للحد من المخاطر التي تهـدد نظم معلوماتها المحاسبية الإلكترونية؟

أهداف الدراسة:

تهدف هذه الدراسة إلى التعرف على مخاطر نظم المعلومات المحاسبية الإلكترونية فـي الشركات المالية الأردنية (البنوك وشركات التأمين) وذلك من خلال تحقيق الأهداف الفرعيـة التالية :-

١- التعرف على طبيعة المخاطر التي تهدد نظم المعلومـات المحاسـبية الإلكترونيـة فـي الشركات المالية الأردنية .

٢- التعرف على درجة تكرار المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الأردنية.

٣- التعرف على إجراءات الحماية التي تتبعها الشركات المالية الأردنية للحد من المخـاطر التي تهدد نظم معلوماتها المحاسبية الإلكترونية.

أهمية الدراسة:

تنبع أهمية الدراسة من النقاط التالية:

١- أن نظم المعلومات المحاسبية الإلكترونية تتعرض للعديد من المخاطر التـي تهـدد صـحة البيانات المالية المحاسبية وموثوقيتها وسريتها وتؤثر في ملاءمة البيانات التي توفرها تلك النظم، لذا يعد تحديد هذه المخاطر بطريقة علمية مدروسة ومنظمة أداة فاعلة في تعزيز حمايـة الـنظم

المحاسبية للبنوك وشركات التأمين الأردنية، وتعزيز ثقة أصحاب المصالح ، ومن ثم الحفاظ على الاقتصاد الوطني وتنميته.

٢- إحتمالية الخلط وعدم التمييز بين مخاطر أمن نظم المعلومات وعدم كفاية إجراءات الحماية لأمن تلك النظم، لذا فإن هذه الدراسة تعنى بالتمييز بين المخاطر التي تعتبر صفة أصيلة في أي نظام معلومات الكتروني، وبين أهم إجراءات حماية تلك النظم الإلكترونية.

٣- ندرة الدراسات في هذا المجال، حيث تعتبر هذه الدراسة (في حدود علم الباحث) من الدراسات القليلة من نوعها التي تطبق على البنوك وشركات التأمين الأردنية، وبالتالي قد تمكن البنوك وشركات التأمين من الإستفادة من نتائجها في تطوير أدائها فيما يتعلق بالسيطرة على المخاطر؛ مما يعزز دورها في المجتمع وزيادة الثقة في الجهاز المصرفي وقطاع التأمين بشكل عام.

الدراسات السابقة :

يعتبر موضوع أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية من المواضيع الهامة والحديثة، وقد تبين للباحث من خلال مراجعته للأدبيات والدراسات السابقة أن هناك نقص في الدراسات العربية والأجنبية على حد سواء . ومن أهم الدراسات التي وجدها الباحث في هذا المجال :

دراسة (الحلو ، ٢٠٠٠م) بعنوان أثر استخدام نظم تكنولوجيا المعلومات على الخدمات المصرفية المتكاملة في البنوك التجارية الأردنية من منظور القيادات المصرفية .

هدفت هذه الدراسة إلى بيان قدرة البنوك التجارية الأردنية على الإستمرار بالعمل أو التنافس إذا لم تستخدم تكنولوجيا الحاسب الآلي والاتصالات بفاعلية في أداء أعمالها المختلفة ، كما هدفت إلى تقديم صورة عن واقع أنظمة المعلومات والاتصالات المستخدمة في البنوك الأردنية من خلال استقصاء آراء مديري التخطيط الاستراتيجي، ومديري التسويق، ومديري تكنولوجيا المعلومات في هذه البنوك .

وقد خلصت الدراسة إلى العديد من النتائج، من أهمها:

أ- أن الاستثمار في تكنولوجيا المعلومات والاتصالات ، يؤدي إلى خفض التكاليف في البنوك التجارية الأردنية .

ب-أن الاستثمار في تكنولوجيا المعلومات والاتصالات ، يؤدي إلى زيادة أرباح البنوك، وزيادة إقبال المودعين وأعدادهم ، ورفع مستوى الخدمة المقدمة للزبائن ، وإظهارها بشكل لائق ومنافس.

ج - لا تستطيع البنوك أن تستمر في عملها وتوفير الخدمات لعملائها دون استخدام تكنولوجيا المعلومات والاتصالات.

دراسة (خطاب ، ٢٠٠٢) بعنوان : تحليل العوامل المؤثرة على كفاءة وفعالية نظم المعلومات المحاسبية في البنوك التجارية الأردنية .

هدفت إلى التعرف على العوامل المؤثرة على كفاءة وفعالية نظم العلومات المحاسبية في البنوك التجارية الأردنية ، وذلك من خلال بيان مدى تأثير كل من(العوامل البيئية ، العوامل

التنظيمية ، العوامل السلوكية لمستخدمي المعلومات، أجهزة وبرامج الحاسوب ، نماذج القرارات الادارية) على كفاءة وفعالية هذه النظم، كما هدفت الى معرفة مـدى قـدرة نظـم المعلومـات المحاسبية على تلبية إحتياجات البنوك التجارية الأردنية من المعلومات الملائمة .

وتوصل الباحث من خلال نتائج الدراسة إلى العديد من التوصيات للبنـوك التجاريـة الأردنية والتي تتعلق بضرورة الاهتمام بالعوامل البيئية المحيطة عنـد إعـداد وتطـوير نظـم المعلومات المحاسبية وخصوصاً فيما يتعلق بالسوق والمنافسة واللوائح والقـوانين الحكوميـة ، وضرورة فهم وإدراك العوامل التنظيمية وأهمية اللامركزية في الإدارة ومـشاركة المـستويات الإدارية المختلفة في عملية إعداد وتطوير نظم المعلومـات المحاسـبية ، ومراعـاة العوامـل السلوكية لمستخدمي المعلومات والتوعيـة بـأثر المعلومـات الناتجـة علـى سـلوك الأفـراد والمستخدمين لهذه المعلومات ، وضرورة مواكبة التطورات التكنولوجيـة واسـتخدام الأجهـزة والبرامج المتطورة ، وإدراك خصائص جودة المعلومات المحاسبية وتعدد الفئـات المـستخدمة للمعلومات مع تعدد احتياجاتهم .

دراسـة (Whitman,2003) بعنـوان : Enemy at the Gate: Threats to Information Security والتي تمحورت حول عوائق نظم المعلومات، وركزت علـى ثلاثة محاور: الأول يتعلق بحصر التهديدات التي تواجه أمن المعلومات ، والثاني يتعلق بدرجـة خطورة هذه التهديدات ، والثالث يتعلق بعدد مرات حدوثها شهرياً. ولتحقيق ذلك قـام الباحـث بعمل تقييم لمجال أمن المعلومات ، وحصر التهديدات التي تواجه أمن المعلومات ، عن طريـق دراسة مسحية شملت ألف موظف ، أغلبهم من مديري نظم المعلومات، ومديري الأقسام

والمشرفين، وأوضحت الدراسة أن التهديد حقيقي، وخطورته عاليـــة، وأن الأنظمـــة المعرضـــة للتهديد يصعب حمايتها، وأن على الإدارة أن تكون مطلعة أكثر على تهديدات أمن المعلومـــات ، لاسيما وأن هذه المخاطر ملازمة لنظم المعلومات من خلال علاقتها مع البيئة التي تعمل بها .

دراسة (Abu-Musa , 2004) بعنوان : Important Threats to Computerized Accounting Information Systems: An empirical study on Saudi Organizations

وهي دراسة تطبيقية للتعرف على المخاطر الهامة التي تهدد أمـــن نظـــم المعلومـــات المحاسبية الإلكترونية في المنشآت السعودية ، وقد أظهرت نتائج الدراسة أن نسبة عاليـــة مـــن المنشآت التي شاركت في الإستقصاء قد عانت من وجود خسائر مالية كبيـــرة ؛ نتيجـــة بعـــض التعديات على أمن نظم المعلومات المحاسبية فيها سواء من قبل أطـــراف داخليـــة أم أطـــراف خارجية . كما أوضحت الدراسة أن كثيراً من تلك التلاعبات والاختلاسات والتعديات على نظـــم المعلومات المحاسبية قد تم اكتشافها عن طريق الصدفة ؛ نتيجة لعـــدم كفايـــة وفعاليـــة الأدوات والضوابط الرقابية المطبقة ، وأن معظم الاختلاسات والتلاعبات التي تـــم إكتـــشافها قـــد تمـــت تسويتها داخلياً ولم يتم الإفصاح أو التقرير عنها للجمهور حفاظاً على سمعة الـــشركة وتحـــسين صورتها في السوق ، أما فيما يخص مدى إدراك المنشآت السعودية للمخاطر الهامة التي تهـــدد نظم المعلومات المحاسبية ومعدلات تكرار حدوث تلك المخاطر بها، فقد أشارت نتائج الدراســـة الى أن أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشآت السعودية هي : الإدخال المتعمد وغير المتعمد لبيانات غير صحيحة بواسطة موظفي المنـــشآت، إدخـــال فيروسات الكمبيوتر إلى النظام المحاسبي، مشاركة الموظفين في إستخدام نفس كلمة السر،

طمس أو تدمير مخرجات الحاسب الآلي ، الكشف غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الأوراق ، وكذلك توجيه المطبوعات والمعلومات إلى أشخاص غير مخول لهم الاطلاع على تلك المعلومات.

وقد إستفاد الباحث من دراسة أبو موسى في تطوير الإستبانة التي تم استخدامها لغايات جمع البيانات اللازمة لاختبار فرضيات الدراسة والتوصل إلى نتائجها.

دراسة (القطناني ، ٢٠٠٥) بعنوان : الضوابط الرقابية في نظم المعلومات المحاسبية المصرفية المحوسبة دراسة تحليلية في المصارف التجارية الأردنية . وتعد هذه الدراسة إستطلاعاً تهدف في إطارها التطبيقي إلى إستكشاف الوضع الحالي لأنظمة الرقابة الداخلية في المصارف التجارية في الأردن وتقييم درجة متانة وفاعلية الإجراءات والضوابط الرقابية المصممة في أنظمة المعلومات المحاسبية المحوسبة، وتحديد مدى توافق خصائص النظام الرقابي لأنظمة المعلومات المحاسبية المطبقة في المصارف التجارية الأردنية مع المواصفات والمعايير الرقابية المتعارف عليها المعتمدة لدى المنظمات المهنية والمصارف الدولية الريادية .

وقد توصل الباحث إلى أن خصائص النظام الرقابي لنظم المعلومات المحاسبية المحوسبة في المصارف التجارية في الأردن تتوافق بدرجة متوسطة مع الضوابط الرقابية ، مع ملاحظة وجود العديد من جوانب القوة في النظام الرقابي من ناحية ووجود مجموعة من الإختلالات ومظاهر الضعف والقصور في أدوات النظام الرقابي لنظم المعلومات المحاسبية المحوسبة في تلك المصارف. وأنها تنطوي على ضعف وقصور كبيرين في العديد من مكوناتها وأدواتها الرقابية وذلك على مستوى الرقابتين العامة والتطبيقية .

دراسة (البحيصي والــشريف، ٢٠٠٧م) بعنوان : مخاطر نظم المعلومـــات المحاســبية الإلكترونية : دراسة تطبيقية على المصارف العاملة في قطاع غزة .

هدفت الى التعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونيــة فــي المصارف العاملة في قطاع غزة ، والتعرف على أهم الأسباب التي تؤدي إلــى حــدوث تلــك المخاطر والإجراءات التي تحول دون وقوعها.

وفي ضوء نتائج الدراسة تم التوصل إلى مجموعة من التوصيات من أهمها :

١- من الضروري أن تدعم الإدارة العليا للمصارف أمن المعلومات لــديها وأن تعمــل علــى إنشاء قسم خاص بتكنولوجيا المعلومات في كافة المصارف وتوفير كادر متخــصص فــي تكنولوجيا المعلومات بحيث يكون له مندوبين في الفروع ذوي خبرة وكفاءة عالية لأجــل العمل على حماية أمن نظم المعلومات المحاسبية لدى المصارف ، وكذلك تطوير قــدرات العاملين لديها في مجال أمن المعلومات وحمايتها .

٢- ضرورة وضع إجراءات تضمن إستمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الازمات، وذلك من خلال إستخدام تجهيزات منيعة أو مرتبة بحيــث تــستطيع اكتــشاف المخاطر قبل حدوثها والحد من وقوعها ، وكذلك العمل على تعمية أو تشفير المعلومــات عند الحفظ والنقل والتخزين على مختلف الوسائط كي لا يتمكن أحد من إختراقها .

٣- وضع ضوابط أمن ورقابة للمعلومات المتداولة بكافة اشكالها ، سواء أكانت ورقية أم إتصالات سلكية ولا سلكية وعبر الإنترنت، والعمل على سن التشريعات اللازمة لأمن

المعلومات والنظم والشبكات المعلوماتية، ووجود خطة حماية أمنية شاملة تؤدي إلـــى خفــض النفقات الناتجة عن توظيف الحلول الجزئية للأمن.

وقد استفاد الباحث من دراسة البحيصي والشريف في تطوير الإستبانة التي تم استخدامها لغايات جمع البيانات اللازمة لاختبار فرضيات الدراسة والتوصل إلى نتائجها.

وما يميز هذه الدراسة عن سابقاتها، أن الدراسات السابقة اســتهدفت التعــرف علــى المخاطر المحتملة التي قد تواجه أو تهدد أمن نظم المعلومات المحاسبية الإلكترونية ومحاولة تطوير قائمة تتضمن أهم المخاطر التي قد تواجه أمن تلك النظم ، ومن ثم محاولة اختبار مدى جوهرية تلك المخاطر من خلال التعرف على حجم الخسائر المالية الناجمة عنها . أما الدراسة الحالية فقد هدفت إلى تحديد مخاطر نظم المعلومات المحاسبية وتحليلها في البنوك وشــركات التأمين الأردنية من خلال تحديد هذه المخاطر والتعرف على درجة تكرارها والإجراءات التي تعمل على تقليل هذه المخاطر التي تؤثر وبشكل مباشر على تــوافر المعلومــات وســريتها وتكاملها .

فرضيات الدراسة :

في ضوء ما تقدم من دراسات سابقة، وتحقيقاً لأهداف الدراسة والإجابة على تساؤلاتها، يمكن صياغة فرضيات الدراسة على النحو التالي :

H01 : لا توجد مخاطر تهدد أمن نظم المعلومات المحاسبيــة الإلكترونية في البنوك وشركات التأمين الأردنية .

H02 : **لا** تعاني نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التأمين الأردنية من تكرار حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية فيها.

H03: لا توجد إجراءات حماية كافية لمواجهة مخاطر أمن نظـــم المعلومـــات المحاسبيـــــــة الإلكترونية في البنوك وشركات التأمين الأردنية.

الفصل الثاني

نظم المعلومات المحاسبية الإلكترونية

- مقدمة

- مفهوم النظام وعناصره

- نظم المعلومات الإلكترونية ووظائفها

- مكونات نظم المعلومات المحاسبية الإلكترونية ومعالمها الأساسية

- تطور نظم المعلومات المحاسبية الإلكترونية في البنوك الأردنية

مقـــــدمة:

أصبحت نظم المعلومات الإلكترونية، تمثل جانباً هاماً مـــن حياتنـــا المعاصـــرة وبخاصـــة إستخدامات هذه النظم التي تعددت وتوسعت لتشمل ميادين العلوم المختلفة .

ويهدف هذا الفصل إلى التعريف بمفهوم النظام وعناصره بشكل عام، ثم التعريـــف بمفهـــوم نظم المعلومات المحاسبية الإلكترونية ووظائفها ومكوناتها الأساسية.

مفهوم النظام وعناصره:

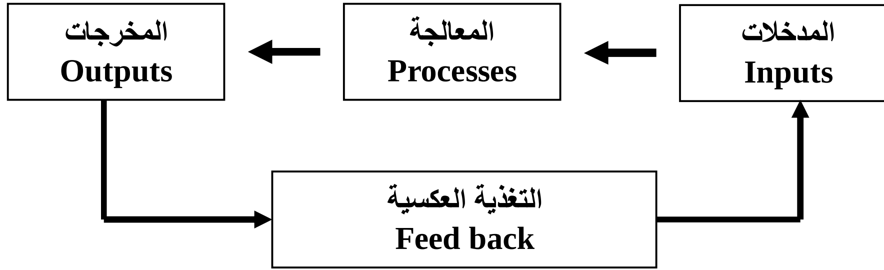
إن كلمة " نظام " (System) من الكلمات المتداولة بشكل واسع في كافة مجـــالات الحياة ، فيستخدم الفرد عادة نظام النقل العام للتنقل من مكان لآخر ، والجسم ذاته يتكـــون مـــن العديد من النظم ، كنظام الجهاز الهضمي ونظام الجهاز التنفسي ، وعلى هذا الأساس تبدو كلمة نظام في ضوء ما تقدم متعددة الاستخدامات والمعاني وعند فحص هذه الاستخدامات والمعـــاني وغيرها نجد أن جميعها يلتقي في جوهر واحد بحيث يتكون كل نظام من هذه النظم من مكونات أساسيـــة تتفـــــاعل فيما بينهـــا وتعمل ضمن ظروف محددة لتحقيق الهـــدف مـــن وجودهـــــا (الدلاهمة، ٢٠٠٧، ص ١٨).

وقد عرّف موسكوف النظام بأنه: "وحدة (Entity) مكونة من مجموعة من الأنظمـــة الفرعية (Subsystem) متداخلة مع بعضها بعضاً وتهدف جميعـــاً إلى تحقيق مجموعة مـــن الأهداف" (ستيفن وسيمكن ، ٢٠٠٠، ص ٢١).

ويرى الباحث أن النظام هو ذلك التجمع اليـــدوي manual system أو الإلكترونـــي electronic systemالذي يتكون من الأجزاء، أوالعناصر، والآلات والوسائل، والإجـــراءات، المرتبطة مع بعضها بعضاً بالإضافة إلى الأفراد بحيث يتم ترتيبهم جميعاً ترتيبا منطقيا مما

يكسبهم عنصر الإنسجام والتكامل والذي يؤدي بهم في النهاية لتحقيق هــدف معــين أو وظيفــة معينة أو مجموعة من الوظائــف أو الأهداف. ويطلق على تلك الأجزاء والعنـــــاصر المكونــة للنظـــام نظماً فرعية subsystems وهي أيضا نظم صغيرة تتكون مــن مكونـــات وأجـــزاء أصغر وتسعى لإنجاز هدف معين والذي يسمى بهدف النظام الفرعي، ويتأثر النظـــام ويــصيبه الخلل وقد يتوقف نهائيا عن العمل في حالة عزل أحد عناصره أو إصابته بتلف.

ويتكون كل نظام من مجموعة من العناصر أو المكونات أو الأجــزاء، وتتــسم هــذه المكونات بالتكامل والترابط والتفاعل والتأثير والتأثر فيما بينها لتحقيق أهداف النظام وهــذه العناصر هي (الدلاهمة ، ٢٠٠٧، ص ص ١٨ – ١٩) :-



الشكل رقم (١) النموذج العام للنظام وعناصره

١- المدخلات (Inputs) وتمثل مدخلات النظام من موارد مادية أو بشرية والتي تــشكل المادة الخام لعملية التفاعل في النظام.

٢- المعالجة (Processing) وهي عملية تحويــل المـــادة الخـــام (المــدخلات) إلـــى مخرجات تحقق أهداف النظام المحددة .

٣- المخرجات (Outputs) وهي نتائج تفاعل مكونات النظـــام وتمثــل نتيجـــة معالجـــة مدخلات النظام .

٤ - التغذية العكسية (Feed Back) وهي عملية إعادة بعض مخرجات النظام إلى النظـــام في صورة مدخلات وتتطلب عملية تصحيح المسارات الخاصـــة فـــي النظـــام توجيـــه ومتابعة تقييم عمليات تنفيذ المخرجات لذا يتطلب فحص فاعلية النظام من خلال النتـــائج والمخرجات الخاصة به.

نظم المعلومات الإلكترونية ووظائفها:

يرتبط التطور في نظم المعلومات الإلكترونية بالتطورات المتسارعة في مجال الحاسبات الآلية التي شاع استخدامها للأغراض العلمية والعسكرية منذ مطلع القرن العشرين، وقد ظهـــرت تطبيقات الحاسوب في منظمات الأعمال في بداية النصف الثاني من القرن العـــشرين وظهـــرت نظم المعلومات المحوسبة computer – Based Information Systems لتعبر عن اســـتخدام الحاسوب في إنتاج المعلومات وحفظها وتوصيلها إلى مستخدميها، ثم ظهر مصطلح تكنولوجيـــا المعلومات (Information Technology (IT وهي وسائل الكترونيـــة لتجميـــع ومعالجـــة وتخزين ونشر المعلومات (Greenstien,&Vasarhely,2000, p21).

وقد أشار البياتي وحسن (٢٠٠١، ص ٤٩) إلى أن جمعية نظم المعلومات الأمريكية عرفت نظام المعلومات الإلكتروني Computer-based Information System بأنه:" نظـــام آلي يقوم بجمع وتنظيم وإيصال وعرض المعلومات لاستعمالها من قبل الأفـــراد فـــي مجـــالات التخطيط والرقابـــــة للأنشطـــة التي تمـــارسهـــا الوحـــدة الإقتصـــادية.

ونظراً لارتباط نظم المعلومات الإلكترونية بكافة الأنشطة والعمليات في المنظمة فإنهـا تقوم بالوظائف الرئيسية التالية (Romny&Steinbart, 2006, p 3):-

١- تجميع وتخزين البيانات عن الانشطة والاهداف المتعددة، والموارد التـي تتـأثر بهـذه الاحداث ، والوكلاء الذين يشاركون في النشاطات المتعددة .

٢- تحويل البيانات الى معلومات تكون مفيدة لصنع القرارات والتي تمكن الادارة من القيـام بوظائف التخطيط والتنفيذ ونشاطات الرقابة .

٣- التزويد بنظام رقابي دقيق لحماية أصول المنظمة والتي تشمل بياناتها ، للتأكـد مـن أن البيانات متوفرة عند الحاجة وأن هذه البيانات دقيقة ويمكن الاعتماد عليها

مكونات نظم المعلومات المحاسبية الإلكترونية ومعالمها الأساسية:

يتكون نظام المعلومات الإلكتروني من المكونات الرئيـسة التاليـة (المجمـع العربـي للمحاسبين القانونيين، ٢٠٠١، ص ٩ – ١٠) :-

أولاً : المدخلات (Inputs)

وهي البيانات الخام التي يتم ادخالها الى الحاسوب لمعالجتها وإنتـــاج معلومات جديدة ويجب تصميم نظام المعلومات المحوسب حتى لا تُجمع البيانات وتدخل أكثر من مرّة واحدة ، ومعنى ذلك أن تُجمع البيانات وتُدخل من جهة واحدة أو مركز المعلومات، ثم يتم إيـصالها الى الجهات المستخدمة المختلفة .

ثانياً : المكونات المادية (Hardware)

وتمثل البنية التحتيـــة لـــنظم تكنولوجيـــا المعلومـــات Information Technology Systems وتتضمن مجموعة من الأجزاء المادية والتجهيزات والمعدات التي يتكون منهـــا جهاز الحاسوب ، والوسائط الاضافية Peripheral Devices والتي يتم تـــشغيلها لانجـــاز مهام ووظائف النظام الحاسوبي ، وهي معدات مادية تستخدم لالتقـــاط ومعالجـــة وتخـــزين البيانات والمعلومات وتوصيلها . وتتضمن خمسة مكونات أساسية هي :

وحـــدات الادخـــال Input Units ، وحـــدة المعالجـــة المركزيـــة (CPU) Central Processing Unit ، وحدات الاخـــراج Output Units ، وســـائط التخـــزين الثانويـــة Secondary Storage Device ، الـــشبكات وأجهـــزة الاتـــصال Networks & Communication Devices

ثالثاً : البرمجيات (Softwares)

وتمثل البرمجيات مجموعة من الأوامر Commands المكتوبة بلغة معينة والتي يـــتم تغذيـــة النظام الحاسوبي وتوجيهه بها لأداء وظائف معينة وتتضمن :

أ- برمجيات النظم Systems Softwares

وهي مجموعة من البرامج تعدها وتجهزها شركات تصميم وتصنيع البرامج وتستخدم فـــي تشغيل الحاســـوب وتـــشمل : نظـــم التـــشغيل Operating Systems ، لغـــات البرمجـــة Programming Languages ، نظـــم إدارة قواعـــد البيانـــات Data – Base Management Systems (DBMS) ، برمجيـــات الاتـــصال Communication Programs

ب - برمجيات التطبيق Application Softwares

وتمثل مجموعة الحزم البرمجية (Software Packages) المصممة بلغة متطورة والتي توجه النظام الحاسوبي لانجاز المهام ومن الامثلة على هذه البرمجيات Microsoft Office والذي يتضمن معالجة النصوص Winword والجداول الالكترونية Excel ومعالج التصاميم Power Point وغيرها.

جـ - البيانات Data

وتمثل المادة الأولية للنظام والتي تجري عليها عمليات التشغيل والمعالجة وهي تختلف عن قواعد البيانات التي تمثل نظم وبرامج تستخدم لادارة البيانات في النظام الحاسوبي.

د - الإجراءات والقواعد Procedures & Rules

وتتضمن منظومة القواعد والمبادئ العلمية وكافة التعليمات وخطط العمل والبرامج التي تحكم التطبيق العملي للنظام والتي يجب اتباعها لجمع وتشغيل وتخزين البيانات المتعلقة بأنشطة المنظمة وتنفيذ الأعمال في النظام الحاسوبي ، وتوفر هذه القواعد مستوى مقبولاً من الملاءمة والمصداقية للنظام.

هـ - الموارد البشرية Prinware

وتتضمن كافة الأفراد الذين يشغلون النظام الحاسوبي ويقومون بالوظائف المختلفة والذين تتكون منهم ادارة نظم المعلومات ويشمل ذلك مدير دائرة الحاسوب Manager ومحللي النظم Analysts Systems ومصممي النظمSystems Designers والمبرمجين Programmers ومشغلي الأجهزة Computer Operators ، ومدخلي البيانات Data Entering ولجنة المراقبة Control Group .

ويعتبر النظام المحاسبي أحد المكونات الاساسية لنظام المعلومات الادارية الكلي فـــي الوحدة الاقتصادية والذي يتألف من مجموعة من الأنظمة الجزئية للمعلومات كنظام التـــسويق ، ونظام التكاليف ، ونظام الانتاج ، ونظام الافراد وغيرها.

ويختص النظام المحاســبي بجمــع (Accumulating) وتبويــب (Classifing) ومعالجـــــة (Processing) وتحليـــــل (Analysing) وتوصـــــيل (Communicating) المعلومات المالية الملائمة لاتخاذ القرارات الى مستخدميها ، أي أنه يتــضمن جميــع الأنــشطة المطلوبة لتزويد الادارة بالمعلومات الملائمة التي تحتاجها في التخطيط والرقابة والتقرير حـــول الظروف المالية والتشغيلية للمنشأة ، ويقوم النظام المحاسبي بجمع البيانات وتنظيمها وتخزينهـــا ومعالجتها يدوياً أو آلياً وعرضها في شكل بيانات خام ، بيانات محللة ، معارف، .. الخ ، وبـــأي من الوسائل النصية والمرئية والصوتية (ستيفن وسيمكن، ٢٠٠٠، ص ٢١ – ٢٥).

ويتكون النظام المحاسبي من مجموعة من الأجزاء والأنظمة الفرعية التـــي تـــرتبط بعضها ببعض وتعمل كمجموعة واحدة تتداخل العلاقات بينها وبين النظام الـــذي يـــضمها وهذه المكونات عبارة عن (Romny&Steinbart, 2006, p7):-

١- الموظفين أو الاشخاص الذين يديرون النظام المحاسبي وينفذون العديد من الوظائف.

٢- الإجراءات والإرشادات بشقيها اليدوي والآلي والمتضمنة جمع ومعالجة وتخزين الأنـــشطة الخاصة بالمنظمة.

٣- البيانات عن المنظمة وإجراءات العمل.

٤- البرامج المحاسبية التي تستخدم لمعالجة بيانات المنظمة.

٥- معلومات عن البنية التحتية التكنولوجية والتي تشمل أجهزة الكمبيوتر ، وأجهزة شبكات الاتصال المستخدمة لجمع ومعالجة ونقل البيانات والمعلومات والرقابة الداخلية وقياس السرية لوقاية البيانات في نظام المعلومات المحاسبي.

تطور نظم المعلومات المحاسبية الإلكترونية في البنوك الأردنية:

أدى الإبداع الإنساني في مجال تكنولوجيا المعلومات ونظم الإتصالات وزيادة حدة المنافسة الناتجة عن عولمة الإقتصاد والأسواق المفتوحة إلى تغيرات جذرية في مختلف جوانب الحياة المعاصرة، وقد استجابت منظمات الأعمال لهذه التطورات بنسب متفاوتة، إلا أن حركة القطاع المالي كانت ولا تزال الأكثر إستجابة لهذه التطورات التي تتطلب منها التوسع في استخدام تكنولوجيا المعلومات وتطوير الأنظمة المعلوماتية وخاصة نظم المعلومات المحاسبية الإلكترونية لمواكبة التطورات التقنية والتكنولوجية والهندسية في مجال تكنولوجيا المعلومات (IT) (الشيخ، ٢٠٠٢، ص ٧).

وقد أدرك المشرع الأردني أهمية تحول البنوك الأردنية من النظم اليدوية التقليدية إلى المعالجة الإلكترونية للبيانات وأهمية إستخدام تكنولوجيا المعلومات والنظم المحوسبة في جمع وتشغيل وتخزين البيانات وإنتاج المعلومات وعرضها حيث إعتبرت المادة (٩٢) من قانون البنك المركزي الأردني رقم (٢٨) لعام ٢٠٠٢م، أن البيانات الإلكترونية أحد أدوات الإثبات في قضايا البنوك شريطة الإحتفاظ بصورة عنها كالمصغرات الفيلمية، وأجاز إستخدامها كدليل للإثبات المحاسبي بدلاً من الدفاتر والسجلات المحاسبية التي نص عليها قانون التجارة ساري المفعول في المؤسسات التي تستخدم النظم التقليدية (القطناني، ٢٠٠٥، ص ٥٣).

يمكن تقسيم مراحل تطور نظم المعلومات المحاسبية في البنوك التجارية الأردنية إلى ثلاث مراحل على النحو التالي (القطناني، ٢٠٠٥، ص ص ٥٣ – ٥٥):

- المرحلة الأولى (إستخدام الالآت التقليدية / ما قبل ١٩٧٠م):

خلال هذه الفترة والتي تمتد منذ نشأة البنوك في الأردن وحتى نهاية العقد السادس من القرن العشرين كانت البنوك الأردنية تستخدم النظام اليدوي التقليدي والذي يعتمد على بعض الالات والحاسبات التقليدية ومسك الدفاتر والسجلات والبطاقات السائبة لخدمة أغراض التشغيل اليومي للبيانات والعمليات المصرفية وإعداد القوائم والتقارير المحاسبية.

- المرحلة الثانية (حوسبة نظم المعلومات المصرفية / ١٩٧٠م – ١٩٩٠م):

يمثل العقد السابع من القرن العشرين (١٩٧٠م – ١٩٨٠م) مقدمات أولية لميلاد أنظمة محاسبية محوسبة في البنوك الأردنية، ويعتبر البنك العربي من أوائل البنوك العربية التي أدخلت الحاسوب لاستخدامه في أنشطتها وعملياتها المصرفية حيث تم تأسيس أول مركز للحاسوب في عمان أواخر عام ١٩٧٢م وتم تشغيله لخدمة الجمهور في المركز الرئيسي للبنك العربي ثم تتابع جهد الإدارة في مكننة العمليات المصرفية وحوسبتها وفي عام ١٩٨٣م تم إعتماد نظام الميكروفيش لتوثيق العمليات المصرفية وتدقيق التواقيع.

أما بنك الإسكان للتجارة والتمويل فقد أدخل الحاسب الآلي لتنظيم عملياته المصرفية خلال الفترة (١٩٧٨م – ١٩٨٠م) وتم التعامل المباشر مع الجمهور خلال العام ١٩٨١م.

كما يعتبر عام ١٩٧٨م بداية إنطلاق النظام الحاسوبي في كل من البنك الأهلي الأردني وبنك الأردن وبنك الاستثمار العربي الأردني ، وبدأ العمل على حوسبة النظام المحاسبي ونظم

المعلومات في البنك الأردني الكويتي عام ١٩٧٩م، وبنك الأردن والخليج وبنك الإنماء الصناعي عام ١٩٨١م وفي البنك الإسلامي الأردني عام ١٩٨٩م، ومع نهاية العقد الثامن وبداية العقد التاسع من القرن العشرين أصبحت جميع البنوك التجارية في الأردن تقدم خدماتها المصرفية بإستخدام الحاسوب.

- المرحلة الثالثة (إستخدام تكنولوجيا المعلومات في تطوير الصناعة المصرفية / ١٩٩٠م وحتى الآن):

في هذه المرحلة أصبحت جميع البنوك العاملة في الأردن تستخدم نظم المعلومات المحوسبة لتنظيم وإدارة عملياتها وتقديم خدماتها بصورة متكاملة، كما شاع إستخدام أشكال جديدة من التقنيات الآلية في العمل المصرفي كالبطاقات المصرفية الإئتمانية مثل Master Card , Visa Card والصراف الآلي (ATM) وظهر البنك الناطق (Phone Bank) والبنك الخلوي (Mobile Bank) واستخدام البريد الإلكتروني وغيرها من الخدمات المصرفية الإلكترونية.

الفصل الثالث

أمن المعلومات الإلكترونية ومخاطرها وإجراءات حمايتها

- مقدمة

- مفهوم أمن المعلومات الإلكترونية ومكوناته

- المخاطر التي تواجه المعلومات الإلكترونية وإجراءات حمايتها

أولاً: مخاطر خرق الحماية المادية وإجراءات حمايتها

ثانياً: مخاطر خرق الحمايـــــة المتعلقة بالأشخاص

وشؤون الموظفين وإجراءات حمايتهـــــا.

ثالثاً: مخاطر خرق الحماية المتعلقة بالإتصـــــالات

والمعطيـــــــــات وإجراءات حمايتهـــــا.

مقـــــــــدمة:

تتعرض المعلومات للعديد من المخاطر في مراحل الجمع والمعالجة والإسترجاع وفـــي مرحلة النقل والتبادل وفي مرحلة التخزين ، وهذه المخاطر تختلف تبعـــا لاخـــتلاف مراحـــل التعامل معها إذ أن لكل مرحلة مخاطرها ووسائل حمايتها الخاصة في عالم يعتمد يوماً بعد يـــوم على تقنية المعلومات.

مفهوم أمن المعلومات الإلكترونية ومكوناته:

أمن المعلومات ، من الناحية النظرية، هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومـــــات من المخاطر التي تهددها من انشطة الاعتداء عليها ومن الناحيـــة التقنية ، هو الوسائل والأدوات والإجراءات اللازم توفيرها لـــضمان حمايـــة المعلومـــات مـــن الأخطار الداخلية والخارجية (عرب ، ٢٠٠١، ص ٣٥).

وحول مكونات أمن المعلومات الإلكترونية فقد أشار الغثبر (٢٠٠٩م، ص ٧) إلـــى أن أمن المعلومات يتكون من ثلاثة مكونات على درجة واحدة من الأهمية، وهذه المكونات هي:

أ- سرية المعلومات (Information Confidentiality) : وهذا الجانب يـــشمل كـــل التدابير اللازمة لمنع إطلاع غير المصرّح لهم على المعلومات الحساسة أو السرية.

ب- سلامة المعلومات (Information Integrity) : ويشمل إتخـــاذ التـــدابير اللازمـــة لحماية المعلومات من التغيير .

جـــ - ضمان الوصول إلى المعلومات والموارد الحاسوبية (Information Availability) : إن المعلومات تفقد قيمتها إذا كان من يحق له الإطلاع عليها لا يمكنه الوصول إليها ، أو أن الوصول اليها يحتاج وقتاً طويلاً.

المخاطر التي تواجه المعلومات الإلكترونية وإجراءات حمايتها:

تتبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة على حد سواء، والتي قد ترد من مصادر داخلية أو خارجية، ومن أهم المخاطر :-

أولاً : مخاطر خرق الحماية المادية Breaches of Physical security وإجراءات حمايتها:

يمكن تعريف الأمن المادي على أنه: حماية أجهزة الحاسب والبرامج والشبكات والبيانات من الأحداث الفيزيائية التي يمكن أن تسبب خسائر وأضرار للمنشأة، وذلك يشمل حمايتها من الحرائق والكوارث الطبيعية والسطو والتخريب (Lehtinen, 2006, p6).

وهناك العديد من إجراءات الحماية المقترحة لمواجهة مخاطر خرق الحماية المادية، منها (إتحاد المصارف العربية،١٩٩٩م، ص ص ٣٤١- ٣٤٢):

١- وضع أجهزة ومعدات الحاسوب في أماكن آمنة ومناسبة.

٢- عدم السماح بالدخول إلى غرفة الحاسوب إلا للأشخاص المخولين وبموجب تفويض سلطة رسمية.

٣- وجود مدخل واحد أو مدخلين لغرفة الحاسوب ويجب أن تكون الغرفة محكمة الإغلاق ومراقبة جيداً.

٤- أن تكون جدران غرفة الحاسوب مكونة من مادة عازلة مقاومة للحرارة وغير قابلة للإشتعال.

٥- أن لا يكون لغرفة الحاسوب نوافذ مطلة على الخارج لتلافـي وقـوع الاخطـار المحتملة .

٦- إستخدام ID User Card للدخول من خلال نقطة وصول معينة.

٧- إستخدام كلمة مرور بالاضافة إلى ID Card لتلافي مخاطر ضياعها وسرقتها.

٨- إستخدام أدوات التعريف الفسيولوجي كالصورة ، الرمـوز البـصرية ، بـصمة الإصبع ، تحليل الصوت، .... وغيرها من الخصائص الفيزيائية المميزة.

٩- إستخدام سجل الزوار والتوقيع عند الدخول وعند الخروج وتحديد الأمـاكن التـي يقومون بزيارتها .

١٠- إستخدام أنظمة التنبيه وأجهزة الإنذار للإعلان عن الوصول غير المصرح به .

١١- تقييد الوصول الى خطوط الهاتف ، الأجهزة الطرفية ، الحواسيب.

١٢- تنزيل قفل على الكمبيوتر ومعدات الحاسوب الأخرى بحيث يغلق مباشـرة عنـد محاولة الدخول غير المصرح بها .

١٣- إستخدام الدوائر التلفزيونية (الكاميرا) والـصور الجانبيـة Profiling للرقابـة وضبط محاولات الدخول إلى غرفة الحاسوب.

١٤- إستخدام الوسائل التقليدية للحماية ومن ذلك:-

- إستخدام العناصر البشرية للحراسة .

- وضع الحواجز المادية والأبواب والتأكد من إحكام غلق غرفة الحاسوب ومواقع التشغيل.

- إستخدام الاقفال الإلكترونية والكهربائية.

ثانياً :مخاطر خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين Breaches of Personnel Security وإجراءات حمايتها:

تعد المخاطر المتصلة بالأشخاص والموظفين ، وتحديداً المخاطر الداخلية منها، واحدة من أهم المخاطر لدى جهات أمن المعلومات ، إذ ثمة فرصة لأن يحقق أشخاص من الداخل ما لا يمكن نظرياً أن يحققه أحد من الخارج ، وتظل أيضا مشكلة صعوبات كشف هؤلاء قائمة ان لم يكن ثمة نظام أداء وصلاحيات يتيح ذلك .

وعموماً فإن هناك تنوع في هذه المخاطر، نذكر منها :

١- التخفي بإنتحال صلاحيات شخص مفوض Masquerading :- والمقصود هنا الدخول الى النظام عبر إستخدام وسائل التعريف العائدة لمستخدم مخول بهذا الاستخدام عن طريق إستراق النظر أو نحو ذلك من الأساليب التي تتواجد في بيئة العمل الداخلي وتتيح الحصول على كلمات المرور أو وسائل التعريف (Lehtinen, 2006, p12).

٢- الهندسة الاجتماعية Social Engineering ويرجع هذا الإسلوب إلى أنشطة الحصول على معلومات بإستغلال الشخص أحد عناصر النظام – أشخاصه – بإيهامه بأي أمر يؤدي الى حصول هذا الشخص على كلمة مرور أو على أية معلومة تساعد في تحقيق إعتدائه ، وأبسط مثال أن يتصل شخص بأحد العاملين ويطلب منه كلمة سر النظام تحت زعم أنه من قسم الصيانة أو قسم التطوير أو غير ذلك(الغثبر ، ٢٠٠٩م، ص ١٦).

٣- الإزعاج والتحرش Harassment :- وهي تهديدات يجمعها توجيه رسائل الازعاج والتحرش وربما التهديد والإبتزاز أو في أحيان كثيرة رسائل المزاح على نحو يحدث

مضايقة وإزعاجا بالغين وليست حكرا على البريد الإلكتروني بل تستغل مجموعـات الحـوار والأخبار والنشرات الإلكترونية في بيئة الإنترنت والويب(عرب،٢٠٠١،ص٣٥).

٤- قرصنة البرمجيات Software Piracy وقرصنة البرامج تتحقق عن طريـق نـسخها دون تصريح أو إستغلالها على نحو مادي دون تخويـل بهـذا الإسـتخدام ، أو تقليـدها ومحاكاتها والإنتفاع المادي بها على نحو يخل بحقوق المؤلف(عرب،٢٠٠١،ص٣٥).

وهناك العديد من إجراءات الحمـايـة المقترحة لمواجهة مخاطر خرق الحمـايـة المتعلقة بالأشخاص من الداخل والتي تتمثل في كافة الضوابط والإجراءات المتعلقـة بفـصل الوظـائف بين إدارة نظم المعلومات والأقسام المستفيدة أو ذات العلاقة وفصل وتقسيم الواجبات وتحديد المسؤوليات في دائرة الحاسوب نفسها من أجل تقليل مخاطر الخطأ والغش.

ويمكن تحديد هذه الضوابط على النحو التالي :-

١- إختيار وتدريب العاملين: يعتبر العنصر البشري المكون الأكثر أهميـة فـي إدارة نظم المعلومات وأنظمة الرقابة الداخلية فالموظف الذي يتمتع بالنزاهة الأخلاقيـة والسلوكية يغني عن الكثير من الإجراءات والضوابط الرقابية.

٢- تدوير العمل وإجازات العاملين: يجب أن يتم منح العاملين فـي دائـرة الأنظمـة إجازاتهم السنوية على دفعات لا تقل عن إسبوع بإستثناء الحالات الطارئة ، كمـا يجب تغيير مواقع عمل الموظفين في الـدائرة بـصورة مـستمرة مـع مراعـاة اعتبارات الخبرة والتخصص وحسب الحالة وتوفر البديل.

٣- دليل العمل: يعتبر دليل العمل بمثابة المرشد والمرجع لإجراءات العمل وبالتالي فإن الإهتمام بإعداد دليل عمل يتضمن تحديداً واضحاً لكافة الوظائف والمهام وتحديداً متسلسلاً للإجراءات العملية التي يجب إتباعها لإنجاز هذه الوظائف والصلاحيات التي تتمتع بها كل وظيفة من الوظائف داخلياً وخارجياً بما في ذلك الوظائف في إدارة الأنظمة يعتبر أحد أهم الادوات والإحتياجات الرقابية التي يجب الإهتمام بها (الشيخ ، ٢٠٠٢، ص ٤).

٤- فصل الوظائف المتعارضة بين إدارة نظم المعلومات والإدارات الأخرى: بغض النظر عن الهيكل التنظيمي لإدارة نظم المعلومات وطبيعة التقسيم الوظيفي لها فإن القاعدة الأساسية التي يجب مراعاتها تتمثل في ضرورة الفصل بين الوظائف المتعارضة في هذه الدائرة بحيث (توماس ، ١٩٨٩م، ص ٤٤١):

أ- لا يسمح للمبرمح باستخدام وتشغيل البرنامج المعد من قبله لان معرفته بالبرنامج تمكنه من التلاعب.

ب - الحد من تدخل مشغل الجهاز في إجراء التعديلات دون الحصول على تصريح بذلك ومراقبة تدخلاته.

جـ- الفصل بين وظيفة محلل النظم والمبرمج بحيث لا يتم تركيز إجراءات إعداد البرنامج لدى شخص واحد.

د- الفصل بين وظيفتي المبرمج ومحلل النظم ووظيفة أمين المكتبة ذلك أن وصول أي منهما إلى مكتبة الحاسوب تمكنه من إجراء عمليات غير مرخصة .

هـ - الفصل بين وظيفة الرقابة والوظائف الأخرى لتمكين لجنة الرقابة من القيام بفحص مراقبة العمل بشكل محايد.

وهناك العديد من الإجراءات الإدارية التي يمكن أن تقوم بها الإدارة للحد من وقوع الأخطاء والمخالفات في إدارة نظم المعلومات منها(الشيخ ، ٢٠٠٢، ص ٥) :-

- فحص واختبار البرنامج المعد من قبل مبرمج آخر
- عدم السماح بتشغيل الأجهزة خارج وقت العمل الرسمي إلا بموافقات أصولية.
- منح الموظفين إجازاتهم السنوية دفعة واحدة وبصورة اجبارية وإحلال موظفين آخرين مكانهم ويساعد ذلك في إكتشاف حالات الغش والتلاعب.
- إستخدام جهاز كمبيوتر خاص لكل مستخدم مع تحديد رقم حساب خاص للمستخدم وربطه برقمه السري.

ثالثا :- مخاطر خرق الحماية المتصلة بالإتصالات والمعطيات Breaches of Communications and Security وإجراءات حمايتها:

يقصد بهذه المخاطر الأنشطة التي تستهدف المعطيات والبرمجيات ذاتها وتشمل مجموعتين:-

- هجمات المعطيات Data Attacks وتتضمن (عرب، ٢٠٠١م،ص ٤٢):

١- النسخ غير المصرح به للمعطيات Unauthorized Copying of Data:- وهي العملية الشائعة التي تستتبع الدخول غير المصرح به للنظام ، حيث يمكن الاستيلاء

عن طريق النسخ على كافة أنواع المعطيات ، وهنا تشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها .

٢- تحليل الاتصالات Traffic Analysis :- الهجوم هنا ينصب على دراسة أداء النظام في مرحلة التعامل ومتابعة ما يتم فيه من إتصالات وإرتباطات بحيث يستفاد منها في تحديد مسلكيات المستخدمين وتحديد نقاط الضعف ووقت الهجوم المناسب وغير ذلك من مسائل يجمعها فكرة الرقابة على حركة النظام بغرض تيسير الهجوم عليه .

٣- القنوات المخفية Covert Channels :- وهي عملياً صورة من صور اعتداءات التخزين ، حيث يخفي المقتحم معطيات أو برمجيات او معلومات مستولى عليها كأرقام بطاقات ائتمان في موضع معين من النظام ، وتتعدد أغراض الاخفاء ، فقد تكون تمهيدا لهجوم لاحق أو تغطية اقتحام سابق أو مجرد تخزين لمعطيات غير مشروعة.

- هجمات البرمجيات Softwares Attacks وتتضمن (الغشبر،٢٠٠٩م، ص ص ٦٧ – ٦٩) :

١- المصائد أو الأبواب الخلفية Trap Doors :- الأبواب الخلفية ثغرة أو منفذ في برنامج يتيح للمخترق الوصول من خلاله إلى النظام ، إنه ببساطة مدخل مفتوح تماماً كالباب الخلفي للمنزل الذي ينفذ منه السارق .

٢- السرقة أو إختلاس المعلومة أو الاستخدام اللحظي (سرقة او اختطاف الجلسات) Session Hijacking :- والمقصود أن يستغل الشخص إستخداماً مشروعا من قبل غيره لنظام ما ، فيسترق النظر أو يستخدم النظام عندما تتاح له الفرصة لإنشغال

المستخدم دون علمه ، أو أن يجلس ببساطة مكان مستخدم النظام فيطلع علـــى المعلومـــات أو يجري أية عملية في النظام .

٣- الهجمات عبر التلاعب بنقل المعطيات عبر أنفاق النقل Tunneling :- أنفاق النقل في الأصل طريقة تقنية مشروعة لنقل المعطيات عبر الشبكات غير المتوافقة، لكنها تـــصبح طريقة إعتداء عندما تستخدم حزم المعطيات المشروعة لنقل معطيات غير مشروعة .

٤- الهجمات الوقتية Timing attacks وهي هجمات تتم بطرق تقنية معقـــدة للوصـــول غير المصرح به الى البرامج أو المعطيات ، وتقوم جميعها على فكرة اســـتغلال وقـــت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام .

٥- البرمجيات الخبيثة Malicious Code كالفايروسات Viruses وحـــصان طـــروادة Trojan Horse والدودة الإلكترونية ً Warms والسلامي Salamis والقنابل المنطقية Logic Bombs :- الجامع المشترك بين هذه البرمجيات انها برمجيات ضارة تـــستغل للتدمير سواء تدمير النظام او البرمجيات او المعطيات او الملفات او الوظائف او تستثمر للقيام بمهام غير مشروعة كانجاز احتيال أو غش في النظام

والفيروسات تمثل حرب الهجمات القائمة والشائعة الآن بسبب إستغلال الإنترنـــت وتوفيرها فرصة نشر البرمجيات الضارة حول العالم ، ولم تعد مجرد هجمة تستهدف نظامـــاً بعينه أو تلحق ضرراً بأحد الملفات ، بل عدت هجمات منظمة تلحق خسائر بالملايين.

إجراءات الحماية لمواجهة مخاطر عدم الوصول المنطقـــي Logical Access Controls والتي تشمل كافة الإجراءات والضوابط المصممة لإحكام السيطرة على الوصول إلى المكونـــات المنطقية للنظام ، ويتضمن ذلك البرامج التطبيقية وأنظمة التشغيل وملفات البيانات والمعلومـــات. ويمكن التمييز بين نوعين من الضوابط لأخطار عدم الوصول المنطقي

أ- ضوابط التحكم وضبط الوصول إلى البرمجيات من خلال:

١- كلمة السر Password: وهي وسيلة تهدف الى التحقق من هوية المـــستخدم وتعريفـــه ليتمكن من الوصول إلى النظام وتحديد البرامج والملفات التي يسمح له بالوصول إليهـــا والعمل من خلالها .

٢- تشفير البيانات Cryptography: وهي وسيلة فعالة للتحكم والـــسيطرة علـــى البـــرامج والبيانات لحمايتها وذلك من خلال تحويل البـــرامج والبيانـــات المكتوبـــة والمقـــروءة والمتبـــادلة من النص البسيط (Plain Text) إلى أشكال ورموز غير مفهومة مكتوبة بالشيفرة (Cypher Text) ، ويتطلب تشفير البرامج والبيانات إستخدام برامج إضـــافية ملحقة كمفتاح للشيفرة والرموز ويجب أن لا تكون هذه البرامج متاحـــة إلا للأشـــخاص المصرح لهم باستخدامها (الشيخ ، ٢٠٠٢، ص ٧).

٣- الجدران النارية Firewalls : وهي برمجيات تستخدم لمنع الدخول غير المصرح إلى النظام حيث تشكل الجدران النارية مصدات وحواجز وسطية Buffers لضبط الوصول إلى برمجيات النظام عبر الشبكات(بهلوان،٢٠٠٤م،ص ٥٥)

٤- التسلل الفاحص أو فحص الاختراق Penetration Test: حيث يتم إســتئجار خــدمات شركات القراصنة المتخصصة لتقمص دور المتطفلين الدخلاء (القراصنة) في الدخول إلى النظام للتعرف على نقاط الضعف القابلة للإختراق في منظومة أمن النظام وإبــلاغ إدارة الشركة عنها لمعالجتها وهو بالتالي يزود إدارة الشركة برؤية تقييميــة لــدفاعات الشبكة وقدرتها على منع واكتشاف حالات الوصول غيــر المــصرح إلــى النظــام (بهلوان،٢٠٠٤م،ص ٥٥).

٥- تقنيات الاشعار باستلام الرسالة (إختبــار الــصدى Echo Check): وهــي تقنيــات برمجية تمكن الوحدة المرسلة للبيانات من التأكد من أن الوحدة المتلقية استلمت الرســالة (البيانات المنقولة) كاملة من خلال المــصادقة علــى وصــول البيانــات آليـــــاً (بهلوان،٢٠٠٤م،ص ٥٦).

٦- الإجراءات التنظيمية Organizational Procedures: وتعني أن يكون الوصول الــى البرامج والبيانات ضمن إدارة نظم المعلومات مراقباً ومسيطراً عليه بعناية مــن خــلال الهيكل التنظيمي لدائرة نظم المعلومات وإجراءات الفصل بين الوظــائف التــي ســبقت الاشارة اليها(بهلوان،٢٠٠٤م،ص٥٦).

٧- السياسات والاجراءات Policies & Proceduers: بحيث يتم تطوير وتنفيذ سياسات وإجراءات للتعامل مع أخطاء النظام في مجال البرامج والبيانات وأنظمة التشغيل

وتوضيحها للعاملين بحيث يمكن معالجتها من خلال أنظمة الأمان لاستعادة النظام وإتاحته للمستخدمين(الفائز،٢٠٠٢م، ص ٢٨).

٨- مصفوفة الرقابة على الوصول Access Matrix: يتم برمجة مصفوفة الرقابة على الوصول آلياً في النظام بحيث تتضمن تحديداً لرقم المستخدم وكلمة السر والملفات أو البرامج التي يصرح له الوصول إليها (بهلوان،٢٠٠٤م،ص ٥٧).

ب- ضوابط أمن وحماية عدم الوصول الى الملفات، من خلال(Romney&Steinbart,2006,pp 293 – 294):

١- توفير النسخ الاحتياطية Backup: تلجأ إدارة نظم المعلومات لعمل الملفات الاحتياطية (Backup) لحفظ الملفات والرجوع اليها عند فقدان أو تلف الصور الأصلية للملف.

٢- حفظ الملفات الاحتياطية في مواقع آمنة ومناسبة Saving Backup: بعد إعداد النسخ الإحتياطية لبرامج التشغيل والبرامج التطبيقية وملفات البيانات فإنه يتوجب الإحتفاظ بها في أماكن آمنة خارج مركز معالجة البيانات مع الأخذ بعين الاعتبار العوامل والمؤثرات الطبيعية كالحرارة والرطوبة وغيرها .

٣- إستخدام بطاقات التعريف الأمامية Internal Labels وبطاقات التعريف الخلفية External Labels لتمييز البيانات المحفوظة على وسائط التخزين.

٤- خطة مواجهة الكوارث .Disaster Recovery Plan: وتمثل مجموعة من الإجراءات التي يتم إتباعها لاسترجاع النظام وإتاحته للمستخدمين لمواجهة الحالات التي يتم فيها فقدان النظام نتيجة لوقوع الاحداث غير الطبيعية ومن هذه الاجراءات:

أ- وجود نظام طاقة إحتياطية لتنظيم تدفق الطاقة إلى النظام وتزويده بالطاقة اللازمة عند إنقطاعها .

ب- توفير أجهزة الانذار المبكر وتوفير نظام لإطفاء ومقاومة الحريق.

جـ - توفير شبكة إتصالات إحتياطية لضمان إستمرارية النظام عبر الشبكة .

د- التغطية التأمينية الملائمة للأجهزة والمعدات في دائرة الحاسوب.

هـ- تدريب العاملين على إجراءات خطة مواجهة الكوارث قبل وقوعها .

و- تشكيل لجنة لاستعادة التشغيل في حالة حدوث الكارثة بحيث تقوم بتقييم الضرر وتوفير وتجهيز مواقع التشغيل البديلة وكافة الموارد الضرورية للعودة إلى الحالة الطبيعية.

٥- البرامج المضادة للفيروسات Antivirus: تعتبر الفيروسات من أكبر المخاطر التي تتعرض لها نظم المعلومات وعلى وجه الخصوص النظم الشبكية حيث يقوم قراصنة الكمبيوتر (Hackers) بمحاولات وصول متعمدة لإدخال فيروسات متلفة لأنظمة المعلومات بواسطة إرسالها كمرفقات عن طريق البريد الإلكتروني ، وتتطلب إجراءات رقابة الأمن والحماية إستخدام برامج حديثة ومتطورة لاكتشاف الفيروسات وتحديد هويتها وتطوير البرامج المضادة للفيروسات Antivirus بصورة دائمة لاكتشافها والتخلص منها وعدم إستخدام الاقراص اللينة أو المدمجة الا بعد نسخها والتأكد من خلوها من الفيروسات .

الفصل الرابع

تحليل البيانات واختبار الفرضيات

- مقـــدمة
- مجتمع الدراسة
- أداة جمع البيانات (الإستبانة)
- أساليب تحليل البيانات
- خصائص الأفراد المجيبين على أسئلة الإستبانة
- اختبار الفرضيات

مقـــــدمة :

يهدف هذا الفصل إلى التعريف بمجتمع الدراسة، وأداة جمع البيانات وأســاليب تحليلهــا ومن ثم اختبار الفرضيات.

مجتمع الدراسة:

جاء اختيار قطاع البنوك وشركات التأمين الأردنية كمجتمع لهذه الدراسة إنطلاقاً مــن الأهمية المميزة لهذه الشركات المالية في دفع عمليــة النمــو الإقتــصادي وتحقيــق الرفاهيــة الاقتصادية للمجتمع ، ولكونها أكثر القطاعات إستخداماً لنظم المعلومات المحاسبية الإلكترونيــة التي تسهم في تطوير أساليب توفير المعلومات وتخزينها.

وتكون مجتمع الدراسة من البنوك وشركات التأمين الأردنية حيث بلغ عــدد البنــوك الأردنية (١٥) بنكاً (حسب تصنيف البنك المركزي الأردني في تقريره السنوي رقم (٤٦) لعام ٢٠٠٩م) وعدد شركات التأمين الاردنية (٢٨) شركة (حسب تصنيف هيئــة التــأمين الأردنية في تقريرها السنوي رقــم (٩) لعام ٢٠٠٩م) وقد تــم توزيــع إســتبانة علــى مديري الدوائر المالية في الإدارة الرئيسية لكل بنك وشركة تأمين ، وعليه فقــد بلــغ عــدد الإستبانات الموزعة (٤٣) إستبانة، وبلغ عدد الإستبانات المستردة والمعتمدة لغايات البحــث والتحليل (٣٧) إستبانة أي ما نسبته (٨٦ %) من الإستبانات الموزعة.

أداة جمع البيانات (الإستبانة):-

قام الباحث بتطوير الإستبانتين المستخدمتين في دراسة (البحيصي والشريف، ٢٠٠٧)، (Abu-Musa,2004)، وقد تكونت الإستبانة بعد تطويرها من أربعة أقسام هدف الأول منها إلى جمع بيانات ديموغرافية عن الأشخاص المجيبين على الإستبانات (المؤهل العلمي ، التخصص العلمي ، سنوات الخبرة في مجال العمل الحالي المحوسب ، الشهادة المهنية، عدد الدورات التي حضرها في مجال مخاطر نظم المعلومات الإلكترونية) وذلك للإطمئنان إلى توفر المعرفة اللازمة لدى المجيبين بنظم المعلومات المحاسبية المحوسبة ، وبمحتويات الإستبانة وقدرتهم على إجابة أسئلتها .

أما القسم الثاني فقد هدف إلى معرفة طبيعة المخاطرالتي تهدد نظم المعلومات الإلكترونية .

بينما هدف القسم الثالث من الإستبانة إلى معرفة درجة تكرار حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية .

وهدف القسم الرابع من الإستبانة إلى معرفة إجراءات الحماية التي تقوم بها إدارات البنوك وشركات التأمين الأردنية للحد من حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية.

ويمكن تلخيص أقسام الإستبانة والأسئلة المخصصة لقياس كل متغير من متغيرات الدراسة في الجدول التالي :

جدول رقم (١)

أقسام الإستبانة والأسئلة التي تقيس كل متغير من متغيرات الدراسة

أقسام الاستبانة	المتغير	الاسئلة التي تقيس المتغير
القسم الأول	المؤهل العلمي	(١)
	التخصص العلمي	(٢)
	عدد سنوات الخبرة في مجال العمل المحوسب	(٣)
	الشهادات المهنية	(٤)
	عدد مرات حضور دورات عن مخاطر نظم المعلومات الالكترونية	(٥)
القسم الثاني	طبيعة المخاطر التي تهدد نظم المعلومات المحاسبية الالكترونية	(٦ – ٢٦)
القسم الثالث	درجة تكرار حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الالكترونية	(٢٧ – ٣٠)
القسم الرابع	إجراءات الحماية للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية	(٣١ – ٤٦)

وقد تم صياغة الأقسام الثلاثة الأخيرة من الإستبانة بشكل يساعد على سهولة القياس حيث اعتمد مقياس ليكرت بدرجاته الخمس (موافق جداً ، موافق ، محايد ، غير موافق ، غير موافق إطلاقاً) .

ولاختبار مصداقية نتائج الإستبانة والإرتباط بين أسئلتها تم عرضها على مجموعة من أساتذة الجامعات في الأقسام المحاسبية ، بهدف تحكيمها وإبداء آرائهم حول سلامة صياغتها وترابط فقراتها ، إضافة الى تحليل المصداقية (الثبات) من خلال إحتساب معامل إرتباط (ألفا كرونباخ) لقياس مدى ثبات أداة القياس حيث بلغت σ = ٨٨,٩٩% وهي نسبة جيدة كونها أعلى من النسبة المقبولة ٦٠% .

كما تم إستخدام إختبار (K – S) لإختبار مدى اتباع البيانات للتوزيع الطبيعـــي حيــث كانت قيمة Sig أكبر من (٠,٠٥) مما يدل على إتباع البيانات للتوزيـــع الطبيعـــي، ويلخــص الجدول التالي قيمة Sig لكل قسم من أقسام الإستبانة الثلاثة الأخيرة:

جدول رقم (٢)

قيمة (Sig) لكل قسم من الأقسام الثلاثة الأخيرة للإستبانة

القسم	Sig
الثاني	٠,٩٠٤
الثالث	٠,٦١١
الرابع	٠,٤٢٦

أساليب تحليل البيانات :

لأغراض تحقيق أهداف الدراسة واختبار فرضياتها تم إســتخدام الأســاليب الإحــصائية التالية:

- الإحصاء الوصفي : حيث تم إيجاد بعــض النــسب والتكــرارات والأوســاط الحــسابية والإنحرافات المعيارية للتعرف على خصائص الأشخاص المجيبين على أسئلة الإستبانة.
- تم استخدام إختبار T –test لإختبار فرضيات الدراسة .

خصائص الأفراد المجيبين على أسئلة الإستبانة:-

يلخص الجدول التالي خصائص الأفراد المجيبين على أسئلة الإســتبانة مــن حيــث مــؤهلاتهم وتخصصاتهم العلمية وسنوات خبرتهم وشهاداتهم المهنية.

جدول رقم (٣)

الخصائص الديموغرافية للأفراد المجيبين على أسئلة الإستبانة

السؤال	بدائل الإجابة	التكرار	النسبة المئوية
المؤهل العلمي	دكتوراه	١	%٢,٧
	ماجستير	٨	%٢١,٦
	بكالوريوس	٢٨	%٧٥,٧
المجموع		٣٧	%١٠٠
التخصص العلمي	محاسبة	٢٠	%٥٤,١
	إدارة أعمال	٦	%١٦,٢
	مالية ومصرفية	٥	%١٣,٥
	نظم معلومات ادارية	١	%٢,٧
	أخرى	٥	١٣,٥
المجموع		٣٧	%١٠٠
عدد سنوات الخبرة	أقل من ٥ سنوات	٢	%٥,٤
	من ٥ إلى أقل من ١٠ سنوات	١٣	%٣٥,١
	من ١٠ إلى اقل من ١٥ سنة	١٠	%٢٧
	١٥ سنة فأكثر	١٢	%٣٢,٥
المجموع		٣٧	%١٠٠
الشهادات المهنية	JCPA	٢	%٥,٤
	CPA	-	-
	CFA	١	%٢،٧
	CMA	-	-
	أخرى	١٠	%٢٧
	لا يوجد	٢٤	%٦٤,٩
المجموع		٣٧	%١٠٠
حضور دورات مهنية	لم أحضر أي دورة	١٣	%٣٥,١
	دورة واحدة فقط	٦	%١٦,٢
	دورتان	١	%٢,٧
	٣ دورات	١	%٢,٧
	أكثر من ٣ دورات	١٦	%٤٣,٣
المجموع		٣٧	%١٠٠

يشير الجدول السابق إلى أن النسبة الأكبر من المجيبين (٧٥,٧%) من حملة البكالوريوس والبقية من حملة الماجستير والدكتوراه مما يدل على إهتمام البنوك وشركات التأمين الأردنية بتعيين أصحاب الإختصاص والمعرفة من خريجي الجامعات.

كما نلاحظ أن (٥٤,١%) من المجيبين من حملة تخصص المحـــاسبــــة وأن (١٦,٢%) منهم إدارة الأعمال، وأن (١٣,٥%) من حملة تخصص مالية ومصرفية، وفـــي هذا إشارة إلى أن المديرين الماليين في البنوك وشركات التأمين الأردنية هم مـــن أصـــحاب الإختصاص ومن المؤهلين علمياً .

ويمكننا ملاحظة إرتفاع متوسطات الخبرة للأفراد المجيبين ، حيث بلغت نسبة الذين تزيد خبرتهم عن ١٥ سنة(٣٢،٥%)، ونسبة الذين تتروراح خبرتهم ما بين ٥ إلى أقل مـــن ١٠ سنوات (٣٥%) مما يدل على إرتفاع درجة الخبرة لدى المديرين الماليين في البنـــوك وشركات التأمين الأردنية.

ونلاحظ قلة حصول المديرين الماليين في البنوك وشركات التأمين على الـــشهادات المهنية المتخصصة ، حيث يتبين لنا أن إثنين من العينة لديهم شهادة JCPA، وأن شـــخص واحد فقط لديه شهادة CFA،وعدم وجود أي شخص من حملـــة شـــهادتي CPA و CMA بينما يوجد عشرة أشخاص لديهم شهادات مهنية أخرى مثل شهادة شركة سيسكو الأمريكيـــة في علم الشبكات CCNP وشهادة المحلل الفني المعتمد CTA وشـــهادة المـــدقق المـــالي المعتمد CIA.

أما بالنسبة لعدد الدورات التي حضرها الموظفون للتوعية في مخاطر نظم المعلومات الإلكترونية، فإننا نلاحظ التفاوت في الإهتمام بهذا الأمر، فقد بلغت نسبة الذين لم يحضروا أي دورة في مجال التوعية بمخاطر نظم المعلومات الإلكترونية (٣٥,١%) من العينة ، مما يدل على ضعف الإهتمام بهذا الجانب لدى بعض الشركات المالية الأردنية ، بينما نجد أن هناك إهتماماً لدى البعض الآخر بالتوعية في مخاطر نظم المعلومات حيث بلغت نسبة الذين حضروا أكثر من ثلاث دورات (٤٣,٢٠%).

اختبار الفرضيات:

اختبار الفرضية الأولى:

H01 : لا توجد مخاطر تهدد أمن نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التأمين الأردنية.

يوضح الجدول رقم (٤) نتائج التحليل الإحصائي للأسئلة المتعلقة بطبيعة المخاطر التي تهدد نظم المعلومات المحاسبية الالكترونية ، حيث تبين أن إتجاهات الأفراد المجيبين تميل إلى تدني الموافقة على السؤال (٢١) المتعلق بقيام أشخاص من خارج المنشأة بطمس أو تدمير بنود معينة من المخرجات ، حيث بلغ متوسطه الحسابي أقل من متوسط أداة القياس (٣) بينما اتجاهات الأفراد المجيبين تميل نحو الموافقة على باقي الفقرات وذلك لأن متوسطاتها الحسابية أكبر من متوسط أداة القياس (٣).

كما تبين أن أكثر المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية هو الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين حيث بلغ المتوسط الحسابي لهذا السؤال (٤,٣٥١) وهذا يتفق مع دراسة (Abu-Musa,2004) التي أجريت على المنشآت السعودية حيث تبين أن أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية هو

الإدخال المتعمد وغير المتعمد لبيانات غير صحيحة بواسطة موظفي المنشأة.

جدول رقم (٤)

نتائج قياس طبيعة المخاطر التي تهدد نظم المعلومات المحاسبية الالكترونية في البنوك وشركات التأمين

رقم العبارة	طبيعة المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية	الوسط الحسابي	الانحراف المعياري
٦	الادخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين	٤,٣٥	٠,٧٩
٧	الادخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين	٣,٦٥	١,٣٥
٨	التدمير غير المتعمد (غير المقصود) للبيانات بواسطة الموظفين	٣,٧٦	١,٢٥
٩	التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين	٣,٧٠	١,٤٠
١٠	الوصول غير المشروع (غير المرخص به) للبيانات والنظام بواسطة الموظفين	٣,٩٠	١
١١	الوصول غير المشروع (غير المرخص به) للبيانات والنظام بواسطة أشخاص من خارج المنشأة	٣,٢٠	١,٣٠
١٢	وجود إشتراك للعديد من الموظفين في نفس كلمة السر	٣,٣٠	١,٥٥
١٣	إدخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل البيانات	٣,٨٠	١,٠١
١٤	إعتراض وصول البيانات من أجهزة الخوادم الى أجهزة المستخدمين	٣,٣٨	١,٠٣
١٥	عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الاعمال من قبل الموظفين	٣,٨١	٠,٩٩
١٦	قيام الموظفين أو المستخدمين بطمس أو تدمير بنود معينة من المخرجات	٣,٣٨	١,١٦
١٧	قيام الموظفين أو المستخدمين بإختلاق مخرجات زائفة غير صحيحة	٣,١٦	١,٢١
١٨	عمل نسخ غير مصرح (مرخص) بها من المخرجات	٣,٢٢	١,١١
١٩	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق	٣,٣٠	٠,٩١
٢٠	قيام أشخاص غير مخولين (غير مصرح لهم) بطباعة وتوزيع المعلومات	٣,٤٩	١,١٢
٢١	قيام أشخاص من خارج المنشأة بطمس أو تدمير بنود معينة من المخرجات.	٢,٩٠	١,٣٠
٢٢	تسليم المستندات الحساسة إلى اشخاص لا تتوافر فيهم الناحية الأمنيـــة بغــرض اتلافها أو التخلص منها	٣,٦٢	١,٣٠
٢٣	توجيه المطبوعات والمعلومات الموزعة خطأ الى أشخاص غير مخولين باستلام نسخة منها	٣,٣٨	١,١٦
٢٤	الحصول على مخرجات غير صحيحة بسبب أخطاء في البرمجة	٣,٨١	٠,٨١
٢٥	الكوارث الطبيعية مثل الزلازل ، الحرائق ، الفياضانات، العواصف ، انقطـــاع الكهرباء ، اعطال أنظمة الاتصالات	٤,١٠	٠,٩٥
٢٦	الكوارث غير الطبيعية والتي هي من صنع الانسان مثل الحرائــق المقــصودة، سرقة أجهزة الحاسوب ، التعطيل المتعمد لأجهزة الحاسوب أو الاتصالات	٤,١١	٠,٨١
	جميع المخاطر معاً	٣,٥٨	٠,٧٠

يشير الجدول السابق إلى أن المتوسط الحسابي للأسئلة التي تقيس طبيعة المخاطر التي تهدد نظم المعلومات الإلكترونية مجتمعة هو (٣,٥٨) مما يعني موافقة الأفراد المجيبين على أنه يوجد العديد من المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الأردنية.

وحول أنواع المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الأردنية، فإنه يمكن بيانها في الجدول التالي:

جدول رقم (٥)

أنواع المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية

انواع المخاطر	الوسط الحسابي	الإنحراف المعياري	الترتيب
مخاطر ادخال البيانات	٣,٨٦٠	٠,٩١٢٠	٢
مخاطر معالجة البيانات	٣,٥٦٠	٠,٨٧٠	٣
مخاطر مخرجات الحاسوب	٣,٣٦٠	٠,٨٢٠٠	٤
مخاطر بيئية	٤,٠٩٥	٠,٧٩٧	١

نلاحظ أن المخاطر البيئية هي أكثر أنواع المخاطر من وجهة نظر الأفراد المجيبين على الإستبانة ، وهذا يتفق مع ما ورد في الجدول رقم (٤) حيث أظهر أن أكثر المخاطر بعد الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين هي المخاطر البيئية من كوارث طبيعة أو غير طبيعية وبلغ متوسطها الحسابي (٤,١١%).

ويظهر من الجدول أيضاً أن مخاطر إدخال البيانات تأتي في المرتبة الثانية من أنواع المخاطر وبمتوسط حسابي (٣,٨٦%) يليها مخاطر معالجة البيانات ثم مخرجات الحاسوب والتي تأتي في المرتبة الأخيرة.

ولغايات اختبار الفرضية تم استخدام T-test ويوضح الجدول رقم (٦) نتائج إختبـــار الفرضية الأولى:

جدول رقم (٦)

نتائج إختبار الفرضية الأولى حسب إختبار T-test

المتغير	t المحسوبة	T الجدولية	SIG t	الوسط الحسابي	الانحراف المعياري
طبيعة المخاطر	5,046	2,028	0,000	3,58	0,70

يتضح من الجدول رقم (٦) أن قيمة (**t المحسوبة** = 5,046) أكبر من قيمتهـــا الجدولية ، وتبعاً لقاعدة القرار : تقبل الفرضية (H0) إذا كانت القيمة المحسوبة أقـــل مـــن القيمة الجدولية والقيمة المعنوية (SIG) أكبر من (0,05) ونـــرفض الفرضـــية (H0) إذا كانت القيمة المحسوبة أكبر من القيمة الجدولية والقيمة المعنوية (SIG) أقل مـــن (0,05)، لذا يتم رفض الفرضية العدمية (H0) وقبول الفرضية البديلة (H1) ، وهذا يعني أن هناك العديد من المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الأردنية. وهذا يتفق مع دراســـــة (Whitman, 2003) التـــي ركـــزت علـــى حـــصر التهديدات التي تواجه أمن المعلومات عن طريق دراسة مسحية شملت ألف موظف أغلـــبهم من مديري نظم المعلومات وأوضحت أن التهديد حقيقي وخطورته عالية ، وأن على الإدارة أن تكون مطلعة أكثر على تهديدات أمن المعلومات.

اختبار الفرضية الثانية :

H02 : لا تعاني نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التـأمين الأردنيـة من تكرار حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية فيها.

يوضح الجدول رقم (٧) الأوزان التي تم إعطاؤها لغايات التحليل الإحـصائي للأسـئلة المتعلقة بدرجة تكرار حدوث المخاطر في البنوك وشركات التأمين الأردنية

جدول رقم (٧)

الأوزان التي تم إعطاؤها لغايات التحليل الإحصائي لدرجة تكرار حدوث المخاطر

الخيارات	أكثر من مرة يوميا	مرّة أو أكثر أسبوعياً	مرة أو أكثر شهرياً	مرة أو أكثـر سنوياً	لا يوجد تكرار نهائياً
الوزن	١	٢	٣	٤	٥

وبالتالي كلما إقتربنا من الدرجة (٥) فإن عدد مرات حدوث المخـاطر يـنخفض إلـى درجة إنعدام حدوث المخاطرعند الدرجة (٥) ويزداد عدد مرات حدوث تلـك المخـاطر كلمـا إقتربنا من الدرجة (١).

ويوضح الجدول رقم (٨) نتائج التحليل الإحصائي للأسئلة المتعلقة بدرجـة تكـرار حدوث المخاطر في البنوك وشركات التأمين الأردنية حيث يبين أن أعلى متوسط حـسابي كـان للسؤال (٢٧) المتعلق بمخاطر إدخال البيانات وهذه إشارة إلى إنخفاض درجة تكـرار حـدوث المخاطر حيث يتجاوز متوسطها الحسابي متوسط المقياس (٣) وبالتالي فإن ذلك يدل علـى أن المخاطر تحدث إما مرة أو أكثر سنوياً ولا يوجد تكرار نهائياً .

وأما تكرار حدوث المخاطر البيئة مثل إنقطاع الكهرباء أو إنقطاع الإتصالات والحرائق والكوارث الطبيعية وغير الطبيعية، فهي أكثر المخاطر تكراراً بمتوسط حسابي (١,٥٢٠%).

جدول رقم (٨)

نتائج قياس درجة تكرار حدوث المخاطر في نظم المعلومات المحاسبية الالكترونية

رقم العبارة	درجة تكرار حدوث المخاطر	الوسط الحسابي	الانحراف المعياري
٢٧	مخاطر إدخال البيانات	٣,٧٠	١,٢٠
٢٨	مخاطر تشغيل ومعالجة البيانات	٢,٦٢	١,٠٠
٢٩	مخاطر مخرجات الحاسب الآلي	٢,٤٩	١,٠١
٣٠	المخاطر البيئية	١,٥٢	٠,٦٩
	الإجمالي	٢,٥٨	٠,٧٤

و نلاحظ أن المتوسط الحسابي يعكس معاناة بيئة نظم المعلومات من تكرار حدوث المخاطر بشكل عام في نظم المعلومات المحاسبية الإلكترونية.

ولغايات إختبار الفرضية تم استخدام T-test ويوضح الجدول رقم (٩) نتائج إختبار الفرضية الثانية:

جدول رقم (٩)

نتائج إختبار الفرضية الثانية حسب إختبار T-test

المتغير	**T المحسوبة**	**t الجدولية**	**SIG t**	**الوسط الحسابي**	**الانحراف المعياري**
درجة تكرار حدوث المخاطر	3,418	2,028	0,002	2,58	0,74

يتضح من الجدول السابق أن قيمة (**t المحسوبة** = 3.418) أكبر من قيمتها الجدولية ، وأن القيمة المعنوية (SIG) أقل من (0,05) لذا يتم رفض الفرضية العدمية (H0) وقبول الفرضية البديلة (H1) ، وهذا يعني أن نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التأمين الأردنية تعاني من تكرار حدوث المخاطر التي تهدد أمن معلوماتها.

اختبار الفرضية الثالثة:

H03 : لا توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية في البنوك وشركات التأمين الأردنية .

يوضح الجدول رقم (١٠) نتائج التحليل الإحصائي للأسئلة المتعلقة بإجراءات الحماية التي تتبعها الإدارة للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية ، حيث يبين أن السؤال (٣١) المتعلق بإجراء الحماية المتمثل في توفير نظام أمن للمعلومات في الشركة هو أكثر الإجراءات موافقة بمتوسط حسابي (٤,٧٦٠) ، بينما السؤال رقم (٤٥) المتعلق بإجراء الحماية المتمثل في الإهتمام بدراسة المشاكل الإقتصادية والإجتماعية والنفسية للموظفين هو أقل إجراءات الحماية موافقة وبمتوسط حسابي (٣,٤٦٠) .

جدول رقم (١٠)

نتائج قياس الإجراءات التي تتبعها الادارة للحد من مخاطر نظم المعلومات المحاسبية الالكترونية في البنوك وشركات التأمين

رقم العبارة	إجراءات الحماية المتبعة	الوسط الحسابي	الانحراف المعياري
٣١	توفير نظام أمن للمعلومات في الشركة	٤,٧٦	٠,٤٣
٣٢	قيام الإدارة باصدار قرارات إدارية خاصة لتجنب تهديدات أمن المعلومات	٤,٦٢	٠,٤٩
٣٣	متابعة موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة	٤,٦٧	٠,٥٣
٣٤	وضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد	٤,٥١	٠,٦٩
٣٥	وضع خطة حماية شاملة ومعمقة تشمل إغلاق مناقــذ الاختــراق، التــدقيق فــي الاجراءات الداخلية ، الاحتفاظ بنسخة احتياطية من المعلومات	٤,٧٣	٠,٤٥
٣٦	تطبيق أهداف حماية أمن المعلومات مثل الخصوصية ، تجنب تغيير البيانات غير المصرح به ، وتوفير البيانات في الوقت المحدد	٤,٥١	٠,٧٣
٣٧	تحليل المخاطر الخاصة بأمن المعلومات مثل العائــد المتوقــع مقابــل تكــاليف الاجراءات المضادة	٤,٠٥	٠,٧٤
٣٨	وضع سياسات خاصة بأمن المعلومات تشمل إختيار التقنية المناسبة ، والاجراءات اللازمة لجعل هذه التقنية فعالة	٤,٣٥	٠,٧٩
٣٩	توفير نظام رقابة داخلي فعال في الشركة	٤,٦٢	٠,٥٤
٤٠	توفير الحماية الكافية ضد مخاطر فيروسات الكمبيوتر	٤,٧٠	٠,٤٦
٤١	معالجة الاختراق عند حدوثه وإصلاح الخلل الناتج عنه	٤,٤٩	٠,٦٩
٤٢	الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات	٤,٥١	٠,٦١
٤٣	التوصيف الدقيق للهيكل الوظيفي والاداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في الشركة	٤,٥١	٠,٦١
٤٤	فحص التاريخ الوظيفي والمهني للموظفين الجدد للتأكد من أمانتهم المهنية	٤,١٣	٠,٦٣
٤٥	الإهتمام بدراسة المشاكل الإقتصادية والإجتماعية والنفسية للموظفين	٣,٤٦	١,٠٩
٤٦	توفير الاحتياطات اللازمة حال حدوث الكوارث غير الطبيعية مثــل الحرائــق ، إنقطاع التيار الكهربائي ، تعطل أنظمة الاتصالات	٤,٣٢	٠,٥٨
	الإجراءات مجتمعة	٤,٤٣	٠,٣٩

نلاحظ أن إتجاهات الأفراد المجيبين إيجابية نحو إجراءات الحماية أعــلاه وذلــك لأن متوسطاتها الحسابية أكبر من متوسط أداة القياس (٣) ، كما أن المتوسط العام يبلغ(٤,٤٣)

ويعكس موافقة الأفراد المجيبين على إجراءات الحماية التي تتبعها الإدارة للحد من المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية.

ولغايات اختبار الفرضية تم استخدام T-test ويوضح الجدول رقم (١١) نتائج اختبار الفرضية الثالثة:

جدول رقم (١١)

نتائج إختبار الفرضية الثالثة حسب إختبار T-test

المتغير	t المحسوبة	t الجدولية	SIG t	الوسط الحسابي	الانحراف المعياري
اجراءات الحماية	22,195	2,0281	0,000	4,43	0,39

وفقاً لنتائج الجدول السابق نجد أن قيمة (**t المحسوبة** = 22,195) أكبر من قيمتها الجدولية ، والقيمة المعنوية (SIG) أكبر من (0,05)، لذا يتم رفض الفرضية العدمية (H0) وقبول الفرضية البديلة (H1) ، بما يعني أنه توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التأمين الأردنية.

نتائج الدراسة :

في ضوء تحليل البيانات التي تم جمعها، وفي ضوء اختبار الفرضيات، يمكن تلخيص نتائج الدراسة في النقاط التالية:

١- هناك العديد من المخاطر التي تهدد أمن نظم المعلومات المحاسبية الالكترونية في الشركات المالية الأردنية .

٢- أكثر مخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التأمين الأردنية هو الادخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين.

٣- تشكل المخاطر البيئية أكثر أنواع المخاطر التي تعاني منها الشركات المالية الأردنية يليها مخاطر إدخال البيانات ثم معالجتها وأخيراً مخاطر مخرجات الحاسوب.

٤- تعاني نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التأمين من تكرار حدوث المخاطر التي تهدد أمن معلوماتها .

٥- تعتبر المخاطر البيئية من أكثر المخاطر تكراراً في نظم المعلومات المحاسبية الالكترونية في الشركات المالية الأردنية .

٦- هناك رضى لدى مديري الدوائر في الشركات المالية الأردنية عن مستوى الإجراءات التي تتبعها إدارات شركاتهم للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية .

٧- توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في البنوك وشركات التأمين الأردنية .

٨- صعوبة الإختراق الخارجي لنظم المعلومات المحاسبية الالكترونية .

توصيات الدراسة :

في ضوء نتائج الدراسة، فإن الباحث يوصي بما يلي:

١- من الضروري أن تدعم الإدارة العليا للبنوك وشركات التأمين الأردنية أمن المعلومات لديها وأن تواكب المستجدات المستمرة في هذا المجال.

٢- ضرورة وضع إجراءات تضمن إستمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الأزمات.

٣- تطبيق إستراتيجية الرقابة الوقائية لمنع وقوع الأخطاء أو المخالفات أو الحد منها في المرحلة الأولى من مراحل النظام .

٤- التحقق من صحة المدخلات وسلامتها وصلاحيتها للمعالجة بعد إدخالها للنظام.

قائمة المصادر والمراجع

المراجع العربية

- § إتحاد المصارف العربية ، **التدقيق والأمان والرقابة في ظل الحاسبات الالكترونية**، ط١، ١٩٩٩، : إتحاد المصارف العربية، بيروت
- § البحيصي، عصام والشريف، حرية ،" مخاطر نظم المعلومات المحاسبية الإلكترونية : دراسة تطبيقية على المصارف العاملة في قطاع غزة "، مجلة الجامعة الإسلامية بغزة: سلسلة الدراسات الإنسانية، ١٦، ، ٨٩٥ – ٩٢٣(٢٠٠٧).
- § بهلوان، شريف، " الاحتياطات اللازمة لضمان التغطية الأمنية للشبكات الداخلية والخارجية"، مجلة الكمبيوتر والاتصالات والالكترونيات ، ٢٠، ٥٥ – ٥٧ (٢٠٠٤) .
- § البياتي، هلال وعبد الرازق، علاء ، **المدخل إلى نظم المعلومات الادارية** ، ط ١، ٢٠٠١، : مديرية دار الكتب للطباعة والنشر، العراق.
- § الحلو، برهان ، أثر إستخدام نظم تكنولوجيا المعلومات على الخدمات المصرفية المتكاملة في البنوك الأردنية من منظور القيادات المصرفية، رسالة ماجستير، ٢٠٠٠، جامعة آل البيت، المفرق، الأردن.
- § خطاب، عبد الناصر، تحليل العوامل المؤثرة على كفاءة وفعالية نظم المعلومات المحاسبية في البنوك التجارية الأردنية ، رسالة ماجستير، ٢٠٠٢، جامعة آل البيت ، المفرق، الأردن.

- الدلاهمة، سليمان مـصطفى، **أساسـيات نظـم المعلومــات المحاسـبية وتكنولوجيــا المعلومات**، ط٢، ٢٠٠٧، : مؤسسة الوراق، الأردن.
- ستيفن، أ.موسكوف وسيمكن، مارك ج، **نظم المعلومات المحاسبية لاتخــاذ القــرارات**، ترجمة كمال الدين سعيد وأحمد حجاج ، ط١، ٢٠٠٠، : دار المريخ ، الرياض.
- الشيخ ، عاصم ، "الإستخدامات الإلكترونية في القطاع المصرفي" ، مجلــة الدراســات المالية والمصرفية ، ١٠، العدد ٢، ٤ – ٧ (٢٠٠٢).
- عرب ، يونس، **قانون الكمبيوتر**، ط١، ٢٠٠١، : اتحاد المصارف العربية، لبنان.
- الغثبر، خالد والقحطاني، محمد ، **أمن المعلومـــــــات بلغة ميسرة**، ط ١، ٢٠٠٩، : منشورات جامعة الملك سعود، المملكة العربية السعودية.
- الفائز ، عبد الرضا، "الانترنت : الأمــن والوقايــة"، مجلــة جامعــة عجمــان للعلــوم والتكنولوجيا ، ٧ ، ص ٢٨ (٢٠٠٢).
- القطناني، خالد، الضوابط الرقابية في نظم المعلومات المحاسبية المصرفية المحوسـبة : دراسة تحليلية في المصارف التجارية الأردنيــة ، رســالة دكتــوراه، ٢٠٠٥، جامعــة دمشق، دمشق، سوريا.
- المجمع العربي للمحاسبين القانونيين ، **تقنيــة المعلومــات** ، ط ١، ٢٠٠١، : مطــابع الشمس ، عمان.
- وليم، توماس و هنكي،أمرسون، **المراجعة بين النظرية والتطبيق** ، تعريب احمد حجــاج وكمال الدين سعيد ، ط١ ، ١٩٨٩، : دار المريخ ، الرياض.

المراجع الأجنبية

- Abu-Musa, Ahmad,"Important Threats to Computerized Accounting Information Systems: An Empirical Study on Saudi Organizations", Public Administration Journal, 44, 1 – 65(2004).
- Basel Committee Publications No 40 , Basel Committee on Banking Supervision, 1998, Swiss.
- Boynton,W.C,Kell, W.C, Modern Auditing, 10th ed,2003,John Wiley & Sons INC,NewYork
- Celinas J.Ulric & Sutton G. Steve, Accounting Information Systems 5th ed.,2001, Prentice Hall, USA
- Gordan, Geoffry, Systems Simulation,2nd ed, 1998, Prentice – Hall, USA
- Greenstien, M.&Vasarhely,M, Accounting Information Technology and Businss Solution, 2nd ed, 2000, Mc Graw -Hill, USA.
- Lehtinen, Rick.,Computer Security Basics 2nd ed,2006,O'Reilly Media, Inc, USA.
- Romney, Marshal B., & Steinbart, Paul John, Accounting Information Systems,10th ed , 2006, Prentice-Hall , USA.
- Whitman, Michael, "Enemy at the Gate: Threats to Information Security", Communication of ACM, Journal, 46 , 91 – 95 (2003).
- William F.Messier, Jr., Auditing & Assurance Service 3rd ed.,2003, Mc Graw-Hill, USA
- http://www.cybrarians.info/journal/no9/info-secuirty.htm
- http://www.geindustrial.com/Banking and Financial Institution Access control, copyright 2002.

ملاحق الدراسة

ملحق رقم (١)

الإستبـــــــانة

الجامعة الهاشمية

كلية الاقتصاد والعلوم الادارية

قسم المحاسبة

السيد/ السيدة .... الفاضل / الفاضلة

السلام عليكم ورحمة الله وبركاته

هذه الاستبانة جزء من دراسة ميدانية يقوم بها الباحث لغايات استكمال متطلبات الحصول على درجة الماجستير في المحاسبة والتمويل وتحمل الدراسة عنوان "مخـــاطر نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الاردنيـــة(البنـــوك وشـــركات التأمين)" تهدف الدراسة إلى التعرف على طبيعة المخاطر التي تهدد نظـــم المعلومـــات المحاسبية الإلكترونية في الشركات المالية الأردنية ومعدلات تكرار هذه المخاطر وكيفيـــة ضبطها ومراقبتها لتخفيض حدة الخسائر المحتملة التي قد تنجم عنها.

لذا، آمل منكم منحني جزءاً من وقتكم للإجابة على الأسئلة الواردة فـــي هـــذه الإستبانة، مؤكداً لكم أن كافة المعلومات سيتم التعامل معها بمنتهى السرية وستكون فقـــط لأغراض الدراسة والبحث العلمي، وإن تعاونكم والإجابة على الأسئلة بدقة وموضـــوعية في غاية الأهمية لإنجاح هذه الدراسة ، مع خالص شـــكري وتقـــديري لحـــسن تعـــاونكم وتجاوبكم

الباحث

أمجد يوسف اسماعيل الزعاترة

<u>القسم الأول :- الخصائص الديموغرافية</u>

يرجى وضع إشارة (**P**) أمام رمز البديل الملائم للأسئلة التالية :-

١ - المؤهل العلمي :-

☐ د كتوراه ☐ ماجستير

☐ بكالوريوس ☐ دبلوم كلية مجتمع فما دون

٢ - التخصص العلمي :-

☐ محاسبة ☐ إدارة اعمال

☐ مالية ومصرفية ☐ نظم معلومات ادارية

☐ أخرى (يرجى ذكرها) ....

٣ - سنوا ت الخبرة في مجال عملكم الحالي :-

☐ أقل من ٥ سنوات ☐ من ٥ الى أقل من ١٠ سنوات

☐ من ١٠إلى أقل من ١٥ سنة ☐ ١٥ سنة فأكثر

٤ - الشهادات المهنية :-

☐ JCPA ☐ CPA

☐ CFA ☐ CMA

☐ أخرى (يرجى ذكرها) ....

٥ - عدد الدورات التي حضرتها في مجال مخاطر نظم المعلومات الإلكترونية :

☐ لم أحضر أي دورة ☐ دورة واحدة فقط

☐ دورتان ☐ ثلاث دورات

☐ أكثر من ثلاث دورات

القسم الثاني :- أنواع مخاطر نظم المعلومات الالكترونية

أولاً) مخاطر إدخال البيانات إلى الحاسب الآلي

يرجى وضع إشارة (**P**) أمام درجة موافقتكم على كل عبارة من العبارات التالية والتي تمثل أحد مخاطر إدخال البيانات الى الحاسب الآلي :-

مخاطر ادخال البيانات الى الحاسب الآلي						
الرقم	العبـــــــارة	درجـــة الموافقـــة				
		موافق جدا	موافق	محايد	غير موافق	غير موافق إطلاقاً
	من مخاطر إدخال البيانات إلى الحاسب الآلي:					
٦-	الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين					
٧-	الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين					
٨-	التدمير غير المتعمد (غير المقصود) للبيانات بواسطة الموظفين					
٩-	التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين					

ثانياً) مخاطر تشغيل ومعالجة البيانات المدخلة إلى الحاسب الآلي

يرجى وضع إشارة (**P**) أمام درجة موافقتكم على كل عبارة من العبارات التالية والتي تمثل أحد مخاطر تشغيل ومعالجة البيانات المخزنة في الحاسب الآلي :-

مخاطر تشغيل ومعالجة البيانات المدخلة الى الحاسب الآلي						
الرقم	العبـــــــارة	درجـــة الموافقـــة				
		موافق جدا	موافق	محايد	غير موافق	غير موافق إطلاقاً
	من مخاطر تشغيل ومعالجة البيانات المخزنة في الحاسب الآلي:					
١٠-	الوصول غير المشروع (غير المرخص به) للبيانات والنظام بواسطة الموظفين					
١١-	الوصول غير المشروع (غير المرخص به) للبيانات والنظام بواسطة أشخاص من خارج المنشأة					
١٢-	يوجد هناك اشتراك للعديد من الموظفين في نفس كلمة السر.					
١٣-	إدخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام					
١٤-	اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين					
١٥-	عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل الموظفين					

ثالثاً) مخاطر مخرجات الحاسب الآلي

يرجى وضع إشارة (**P**) أمام درجة موافقتكم على كل عبارة من العبارات التالية والتي تمثل أحد مخاطر مخرجات الحاسب الآلي :-

مخاطر مخرجات الحاسب الآلي						
الرقم	العبـــــــــــــــــــارة	درجـــــة الموافقـــــــة				
		موافق جدا	موافق	محايد	غير موافق	غير موافق إطلاقاً
	من مخاطر مخرجات الحاسب الآلي:					
١٦-	قيام الموظفين أو المستخدمين بطمس أو تدمير بنود معينة من المخرجات					
١٧-	قيام الموظفين أو المستخدمين بإختلاق مخرجات زائفة /غير صحيحة					
١٨-	عمل نسخ غير مصرح (مرخص) بها من المخرجات					
١٩-	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق					
٢٠-	قيام اشخاص غير مخولين (غير مصرح لهم) بطباعة وتوزيع المعلومات					
٢١-	قيام اشخاص من خارج المنشأة بطمس أو تدمير بنود معينة من المخرجات					
٢٢-	تسليم المستندات الحساسة الى اشخاص قد لا تتوافر فيهم الناحية الأمنية بغرض إتلافها أو التخلص منها					
٢٣-	توجيه المطبوعات والمعلومات الموزعة خطأ إلى أشخاص غير مخولين باستلام نسخة منها.					
٢٤-	الحصول على مخرجات غير صحيحة بسبب أخطاء في البرمجة					

رابعاً) مخاطر بيئية

يرجى وضع إشارة (**P**) أمام درجة موافقتكم على كل عبارة من العبارات التالية والتي تمثل أحد المخاطر البيئية للحاسب الآلي :-

الرقم	العبــــــــــــــــــــــارة	درجـــــــة الموافقــــــــــة				
		موافق جدا	موافق	محايد	غير موافق	غير موافق إطلاقاً
من المخاطر البيئية للحاسب الآلي:						
٢٥-	الكوارث الطبيعية مثل الزلازل، الحرائق ، الفيضانات ، العواصف ، إنقطاع التيار الكهربائي ، الأعطال في أنظمة الاتصالات					
٢٦-	الكوارث غير الطبيعية والتي هي من صنع الانسان مثل الحرائق المقصودة ، سرقة أجهزة الحاسوب ، التعطيل المتعمد لأجهزة الحاسوب أو الإتصالات					

القسم الثالث :- درجة تكرار حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الالكترونية

يرجى وضع إشارة (**P**) أمام العبارة التي تمثل درجة موافقتكم على عدد مرات تكرار حدوث مخاطر نظم المعلومات الالكترونية:

أنواع مخاطر نظم المعلومات	درجة تكرار حدوث المخاطر				
	أكثر من مرّة يوميا ًأو بصفة متكررة	مرّة أو أكثر أسبوعياً	مرّة أو أكثر شهرياً	مرّة أو أكثر سنوياً	لا يوجد تكرار نهائياً
٢٧ - مخاطر ادخال البيانات					
٢٨ – مخاطر تشغيل ومعالجة البيانات					
٢٩ - مخاطر مخرجات الحاسب الآلي					
٣٠ - المخاطر البيئية					

القسم الرابع :- إجراءات الحماية التي تتبعها الادارة للحد من المخاطر التي تهدد نظم المعلومات المحاسبية الالكترونية

يرجى وضع إشارة (**P**) أمام درجة موافقتكم على كل عبارة من العبارات التالية والتي تمثل إجراء من الاجراءات التي تقوم بها الادارة للحد من حدوث مخاطر نظم المعلومات المحاسبية الالكترونية :-

إجراءات الحماية المتبعة						
الرقم	العبـــــــــــــــــــارة	درجـــــة الموافقـــــة				
		موافق جدا	موافق	محايد	غير موافق	غير موافق إطلاقاً
من الإجراءات التي تقوم بها الإدارة للحد من حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية:						
٣١-	توفير نظام أمن للمعلومات في الشركة.					
٣٢-	تقوم الإدارة بإصدار قرارات إدارية خاصة لتجنب تهديـدات أمـن المعلومات.					
٣٣-	متابعة موظفي تكنولوجيا المعلومات في تنفيذ إجـراءات الحمايـة المطلوبة					
٣٤-	وضع قواعد خاصة بحماية أمن المعلومـات ومعاقبـة المـوظفين المخلين بهذه القواعد					
٣٥-	وضع خطة حماية شاملة ومعممة تشمل إغلاق منافـذ الاختـراق، والتدقيق في الاجراءات الداخلية والاحتفاظ بنسخة احتياطيـة مـن المعلومات يمكن الرجوع اليها عند الضرورة.					
٣٦-	تطبيق أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد.					
٣٧-	تحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة					
٣٨-	وضع سياسات خاصة بأمن المعلومات تشمل اختيار التقنية المناسبة، والإجراءات اللازمة لجعل هذه التقنية فعالة.					
٣٩-	توفير نظام رقابة داخلي قوي وفعال في الشركة					
٤٠-	توفير الحماية الكافية ضد مخاطر فيروسات الكمبيوتر					
٤١-	معالجة الاختراق عند حدوثه وإصلاح الخلل الناتج عنه					
٤٢-	الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات					
٤٣-	التوصيف الدقيق للهيكل الوظيفي والاداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في الشركة					
٤٤-	فحص التاريخ الوظيفي والمهني للموظفين الجدد للتأكد من أمانتهم المهنية					
٤٥-	الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية للموظفين					
٤٦-	توفير الاحتياطات اللازمة حال حدوث الكوارث غير الطبيعة مثـل الحرائق ، انقطاع التيار الكهربائي ، تعطل أنظمة الاتصالات					

في حال وجود مخاطر أخرى لم ترد في هذه الاستبانة يرجى التكرم بذكرها :-

....

....

....

....

....

مع جزيل الشكر والتقدير لتعاونكم في تعبئة هذه الإستبانة

الباحث

ملحق رقم (٢)

أسماء الأساتذة محكمي الإستبانة

الرقم	إسم المحكم	إسم الجامعة
١	د. فهيم لوندي	الجامعة الهاشمية
٢	أ. د. يوسف سعادة	جامعة العلوم التطبيقية
٣	أ.د. خالد الخطيب	جامعة العلوم التطبيقية
٤	د. محمد رحاحلة	جامعة آل البيت
٥	د. جمال الشرايري	جامعة آل البيت
٦	د. سليمان البشتاوي	جامعة آل البيت
٧	د. غسان المطارنة	جامعة آل البيت
٨	د. عبير خوري	جامعة اليرموك
٩	د. ميشيل سويدان	جامعة اليرموك

ملحق رقم (٣)
أسماء البنوك وشركات التأمين الأردنية
الممثلة لمجتمع الدراسة

الرقم	إسم الشركة	الرقم	إسم الشركة
١	بنك الأردن	٢٠	العربية الألمانية للتأمين
٢	بنك ABC	٢١	التأمين الإسلامية
٣	بنك القاهرة عمان	٢٢	الضامنون العرب
٤	بنك المال الأردني Capital Bank	٢٣	المتوسط والخليج
٥	البنك التجاري الأردني	٢٤	الشرق الأوسط للتأمين
٦	البنك الأردني الكويتي	٢٥	النسر العربي للتأمين
٧	البنك الأهلي الأردني	٢٦	التأمين الأردنية
٨	بنك الإسكان	٢٧	دلتا للتأمين
٩	بنك الإستثمار العربي الأردني	٢٨	القدس للتأمين
١٠	بنك سوستيه جنرال الأردن	٢٩	الأردنية الفرنسية للتأمين
١١	البنك العربي الإسلامي الدولي	٣٠	اليرموك للتأمين
١٢	بنك الإتحاد	٣١	البركة للتكافل
١٣	البنك الإسلامي الأردني	٣٢	المنارة للتأمين
١٤	شركة التأمين العامة العربية	٣٣	الشرق العربي للتأمين
١٥	المتحدة للتأمين	٣٤	الأردنية الإماراتية للتأمين
١٦	الأراضي المقدسة للتأمين	٣٥	الأولى للتأمين
١٧	الإتحاد العربي الدولي للتأمين	٣٦	المجموعة العربية الأوروبية للتأمين
١٨	التأمين الوطنية	٣٧	المجموعة العربية الأردنية للتأمين
١٩	الأردن الدولية للتأمين		

Abstract

Risks of the Electronic Accounting Information Systems
In the Jordanian Financial companies
(Banks & Insurance Companies)

by

Amjad Yousef Ismael AL Zaatreh

Supervisor
Dr. Walid Zakaria Siam
Associate Professor

This study aims to identify the risks facing the electronic accounting information systems in the Jordanian financial companies (banks and insurance companies) and to further identify the frequency of occurrence of these risks and the required protection procedures .

To achieve the objectives of the study , ,the researcher developing a questionnaire which distributed to the financial managers in the banks and insurance companies listed in Amman Stock Exchange in the year 2009 , their number is 15 banks and 28 insurance companies .

The number of distributed questionnaires is 43 . thirty seven questionnaires are collected and credited for the purpose of statistical analysis , i.e. 86% of the total distributed questionnaires . The following results of the study are:

1. There are a number of risks which threaten the electronic accounting information security in the Jordanian Financial companies.
2. The environmental risks constitute the most risky types suffered by the Jordanian financial companies.
3.the electronic accounting information system environment suffers of frequency of occurrence of such risks which threaten the accounting information system .
4. The stakeholders of the Jordanian financial companies are highly concerned to provide a special system for the information security in the company.

In accordance to the results of the study , the researcher recommend the following:

1. Setting the necessary procedures to ensure the continuity and persistence of the work and readiness of the AIS to work in the conditions of conflicts
2. Applying the strategy of preventive control to avoid the occurrence of risks or defaults or to restrict them in the primary phase of the system.
3. Developing the capabilities of the staff working in the field of information security and protection and pay more attention for their engagement in the specialized training courses.